Declaration

I, Atsuko Sato, a member of Hayase & Co. patent attorneys of 13F, Nissay Shin-Osaka Bldg., 3-4-30, Miyahara, Yodogawa-ku, Osaka-shi, Osaka 532-0003 Japan, hereby declare that I am the translator of the attached document and certify that the following is a true translation to the best of my knowledge and belief.

Osaka, this 7th day of October, 2003

Atsuko Sato

Atsuko Sato

[Name of Document] Patent Application

[Reference Number] 2022500219

[Filing Date] September 2, 1998

[Destination] Commissioner, Patent Office

[International Patent Classification] H04N 7/167

[Title of Invention] DATA PROCESSING METHOD, DATA PROCESSING APPARATUS, AND DATA STORAGE MEDIUM

[Number of Claims] 22

[Inventor]

[Address] c/o Matsushita Electric Industrial Co., Ltd, 1006, Oaza Kadoma, Kadoma-shi, Osaka

[Name] Toshiya Takahashi

[Applicant]

[Identification No.] 000005821

[Name] Matsushita Electric Industrial Co., Ltd.

[Patent Attorney]

[Identification No.] 100081813

[Patent Attorney]

[Name] Kenichi Hayase

[Telephone Number] 06(380)5822

[Representation of Fee]

[Ledger No.] 013527

[Amount of Payment] 21,000

[Attached Documents]

[Name of Document] Specification 1

[Name of Document] Drawing 1

[Name of Document] Abstract 1

[Number of General Authorization] 9600402

[Name of Document] Specification

[Title of Invention] DATA PROCESSING METHOD, DATA PROCESSING APPARATUS, AND DATA STORAGE MEDIUM

[Claims]

[Claim 1] A data processing method for storing or transmitting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, wherein

at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of objects are encrypted; and

the respective object data and the scene description data are then stored or transmitted.

[Claim 2] The data processing method of Claim 1, wherein

encryption identifiers each indicating whether or not object data corresponding to any object of the plurality of objects has been encrypted is included in the scene description data, and stored or transmitted.

[Claim 3] The data processing method of Claim 1, wherein

information required for the encryption is included in the scene description data, and stored or transmitted.

[Claim 4] The data processing method of Claim 1, wherein

the scene description data is not encrypted and only

object data corresponding to the objects to-be-protected is encrypted, and these data are stored or transmitted.

[Claim 5] The data processing method of Claim 1, wherein

in encrypting a plurality of object data when a plurality of objects are objects to-be-protected, a plurality of information of different types, which correspond to the respective object data, are used as information required for the encryption.

[Claim 6] The data processing method of Claim 1, wherein

in the encryption process, a type of information required for the encryption is changed with elapse of time.

[Claim 7] A data processing apparatus for storing or transmitting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, said apparatus comprising:

a plurality of data compression means respectively provided for the objects, for compressing respective object data;

multiplexing means for multiplexing the scene description data and the compressed object data output from the data compression means respectively as individual streams and outputting a multiplexed bit stream; and

encryption means for performing encryption for

encrypting individual streams in the multiplexed bit stream which correspond to the objects to-be-protected having copyrights to be protected, to produce an encrypted bit stream, wherein

the encrypted bit stream is output to the data storage medium or the data transmission medium.

[Claim 8] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, wherein

reproduction including decryption of the encrypted data and display of respective object data is performed on the encrypted data depending on whether or not the scene description data and the respective object data have been encrypted.

[Claim 9] A data processing apparatus which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs

reproduction of the encrypted data, the encrypted data being obtained by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, said apparatus comprising:

decryption means for performing decryption for decrypting encrypted scene description data or object data according to a first control signal, to produce decrypted data;

display means for displaying the scene based on the decrypted data according to a second control signal; and

control means for controlling said decryption means and said display means by using the first and the second control signals so that reproduction including decryption of the encrypted data and display of respective object data is performed depending on whether or not the scene description data and the respective object data have been encrypted, when the encrypted data are received.

[Claim 10] A data storage medium which contains a data processing program for making a computer perform data processing for a plurality of object data respectively

corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, wherein

said data processing program makes a computer perform:

a process of encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of objects; and

a process of storing or transmitting the respective object data and the scene description data after the above process.

[Claim 11] A data storage medium for storing digital data used for reproducing a scene, wherein

said digital data includes a plurality of object data respectively corresponding to a plurality of objects which compose the scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, and is obtained by encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected.

[Claim 12] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by

performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data and scene description data which describes how the plurality of objects compose the scene, wherein

only when reproduction-ready state where encrypted object data corresponding to the objects to-be-protected is reproducible is detected,

reproduction of all the object data including decryption of the object data corresponding to objects to-be-protected and display of the respective object data is performed.

[Claim 13] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data and by performing encryption for encrypting at least compressed object data corresponding to objects to-be-protected having copyrights to be protected among the compressed object data and scene description data which describes how the plurality

of objects compose the scene, wherein

only when reproduction-ready state where encrypted object data corresponding to objects to-be-protected is reproducible is detected,

reproduction of all the object data including decryption of the object data corresponding to objects to-be-protected, and decompression and display of the respective object data is performed.

[Claim 14] The data processing method of Claim 13, wherein

the reproduction-ready state is a state where all the encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through a transmission medium.

[Claim 15] The data processing method of Claim 13, wherein

the reproduction-ready state is a state where the scene description data has been read from the storage medium or received through the transmission medium as well as a condition that all the encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through the transmission medium.

[Claim 16] The data processing method of Claim 13, wherein

the reproduction-ready state is a state where the scene

description data has been read from the storage medium or received through the transmission medium as well as a condition that all the object data including encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through the transmission medium.

[Claim 17] The data processing method of Claim 13, wherein

the reproduction-ready state is a state where the scene description data and all the object data which compose the scene have been read from the storage medium or received through the transmission medium.

[Claim 18] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of compressed object data and scene description data which describes how the plurality of objects compose the scene, wherein

in a decompression process of decompressing all compressed object data obtained by performing decryption for decrypting the encrypted data to produce restored object data,

all the restored object data corresponding to objects are written onto reference memories and read from the reference memories; and

all the restored object data are subjected to secondary encryption when it is written onto the memories and the read restored object data is subjected to decryption for decrypting the secondary encryption when it is read from the memories.

[Claim 19] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of compressed object data and scene description data which describes how the plurality of objects compose the scene, wherein

in a decompression process of decompressing all

compressed object data obtained by performing decryption for decrypting the encrypted data to produce restored object data,

the restored object data corresponding to the respective objects is written onto reference memories corresponding to the respective objects and read from the corresponding reference memories as required; and

the restored object data is subjected to secondary encryption when it is written onto the memories and the read restored object data is subjected to decryption for decrypting the secondary encryption when it is read from the memories, the secondary encryption and the decryption being performed independently for each memory.

[Claim 20] A data processing apparatus which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the compressed object data and scene description data which describes how the plurality of objects compose the scene, said apparatus

comprising:

decryption means for performing decryption for decrypting the encrypted data to produce decrypted data;

a plurality of data decompression means respectively provided for the objects, for decompressing compressed object data of the corresponding object included in the decrypted data, to produce decompressed object data; and

a plurality of memories respectively provided for the objects, for storing decompressed object data of corresponding object, wherein

each of said plurality of data decompression means includes an encryption unit for subjecting the decompressed object data to secondary encryption when the decompressed object data is output to the corresponding memory, and a decryption unit for performing decryption for decrypting the secondary encryption on the decompressed object data read from the memory.

[Claim 21] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data including display of an image data, the encrypted data being obtained by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data respectively corresponding to a

plurality of objects which compose a scene and including object data as video data or audio data and scene description data which describes how the plurality of objects compose the scene, wherein

the individual display of image data corresponding to objects to-be-protected having copyrights to be protected is limited.

[Claim 22] A data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data including display of an image data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the compressed object data and scene description data which describes how the plurality of objects compose the scene, wherein

the image data corresponding to objects to-be-protected having copyrights to be protected is displayed only when the compressed object data corresponding to all objects which compose the scene are decompressed.

[Detailed Description of the Invention]

[0001]

[Applicable Field in the Industry]

The present invention relates to a data processing method and a data processing apparatus. More particularly, the present invention relates to a process for transmitting/receiving data in which unauthorized copying of information represented as digital image data, digital audio data, and the other digital data, and the like is limited, measures are taken for protecting the information according to a copyright, and the use of the information under control of accounting is realized.

[0002]

[Prior Art]

As digitization of image data evolves, there is a need for protection of a copyright of an image represented as digital data, since an image quality of the digital data is not degraded if duplicated. In addition, protection of the copyright of the image is closely related to control of accounting on the usage of the image data, and a conditional access method which is put into practical use in digital satellite broadcast is considered as measures taken to protect the copyright of the image data.

[0003]

As an example of a conventional method for protecting the copyright, the above-described conditional access method

for digital satellite broadcast ("Satellite Digital Broadcast System Technology" written by Asada, Inoue, et.al, Matsushita Technical Journal Vol.44, No.1, Feb. 1998), will now be described with reference to figures. In this digital satellite broadcast, a compression scheme and a multiplexing scheme according to MPEG (Moving Picture Experts Group) 2 standard are employed.

[0004]

Figure 9 is a diagram for explaining a conventional conditional access method and showing a data transmission/receiving system which adopts the conditional access method.

The data transmission/receiving system 1000 comprises a data transmission-side apparatus 81 for compressing, multiplexing, and scrambling video data and audio data according to MPEG2 standard and outputting the resulting data, and a data receiving-side apparatus 91 which receives and reproduces scrambled data from the data transmission-side apparatus 81.

[0005]

The data transmission-side apparatus 81 includes an audio encoder 82 for compressing the audio data Dau according to MPEG2 standard and outputting compressed audio data EDau, a video encoder 83 for compressing the video data Dvi according to MPEG2 standard and outputting compressed video

data EDvi, and multiplexing means 84 for packetizing the data outputted from the encoders 83 and 84 respectively such that each of packets has a fixed-bit length, multiplexing the data packets, and outputting a multiplexed bit stream MB.

[0006]

The data transmission-side apparatus 81 further includes a scrambler 85 for scrambling a predetermined portion of the multiplexed bit stream MB by using a scramble key Ksn and outputting a scrambled (encrypted) bit stream SB, a scramble key encryption unit 86 for encrypting the scramble key Ksn by using a work key KW, and a work key encryption unit 87 for encrypting the work key KW by using a master key KMm to generate an encrypted work key KWm.

[0007]

On the other hand, the data receiving-side apparatus 91 includes a work key decryption unit 97 for decrypting the encrypted work key KWm by using the master key KMm to generate the work key KW, a scramble key decryption unit 96 for decrypting the encrypted scramble key Ksn by using the work key KW to generate the scramble key Ksn, and a descrambler 92 for descrambling a scrambled portion of the scrambled bit stream SB outputted from the transmission-side apparatus by using the scramble key Ksn to produce a descrambled bit stream DB.

[0008]

The data receiving-side apparatus 91 still further includes separation means 93 for separating the compressed audio data EDau and the compressed video data EDvi from the descrambled bit stream DB, an audio decoder 94 for decoding the compressed audio data EDau to provide reproduced audio data RDau, and a video decoder 95 for decoding the compressed video data EDvi to provide reproduced video data RDvi.

[0009]

Figure 10 shows a packet structure of the scrambled bit stream SB obtained by scrambling the multiplexed bit stream MB.

The packet 100a of the scrambled bit stream SB includes a header 100, followed by an adaptation field 101 which represents attribute information and the like of the data and a data region called "Pay Load 102" which follows the adaptation field 101. The compressed audio data EDau and the compressed video data EDvi are stored in the Pay Load 102, and the Pay Load 102 corresponds to a scrambled region which has been subjected to scrambling process.

[0010]

By the way, in the above data transmission/receiving system 1000, accounting on the data is controlled, that is, for a charged program which requires a contract and the like, corresponding program data is scrambled so that only a specified viewer which made the contract can view this

program and thereby a kind of copyright protection is provided. Therefore, for the charged program which requires a contract and the like, it is difficult for general viewers to normally reproduce and watch the contents of the program.

[0011]

More specifically, the Pay Load 102 of the packet corresponding to the charged program which is included in the multiplexed bit stream, is scrambled, and thereby general viewers cannot normally watch the program. In addition, to the header 100 of each packet 100a, an identifier indicating whether or not the Pay Load 102 is scrambled is affixed and further, when the Pay Load 102 is scrambled, an identifier indicating whether the scramble key is represented as an odd number or an even number is affixed.

[0012]

Operation will now be described.

When the video data Dvi and the audio data Dau are input to the data transmission-side apparatus 81, the video encoder 83 and the audio encoder 82 compress these data according to MPEG2 standard, to produce the compressed video data EDvi and compressed audio data EDau, respectively. The multiplexing means 84 multiplexes the compressed data EDvi and EDau according to MPEG2 standard such that each of them is divided into a packet having a fixed-packet length, i.e.,

a fixed-bit length.

[0013]

When the multiplexed bit stream MB outputted from the multiplexing means 84 is input to the scrambler 85, the scrambler 85 scrambles the Pay Load 102 of the packet 100a included in the multiplexed bit stream MB, which corresponds to data for which accounting is to be controlled, and outputs accounting-controlled bit stream (scrambled bit stream) SB.

[0014]

Hereinafter, the above scrambling will be explained in detail. Here, a scramble key for performing the above-described scrambling is described as Ks.

As described above, the multiplexed bit stream MB obtained by multiplexing the compressed audio data EDau and the compressed video data EDvi is scrambled, i.e., encrypted, according to the scramble keys Ks and output as broadcast data (scrambled bit stream) SB. At this time, for security, the scramble keys Ks are updated at intervals ranging from several to several-ten seconds. The scramble key Ksn represents time-series data of the scramble keys Ks, i.e., a set of scramble keys Ks updated at regular time intervals.

[0015]

The scramble key Ksn is further encrypted by using the work key KW, and the encrypted scramble key Ksn as well as the broadcast data SB is outputted. At this time, the

scramble key Ksn is transmitted in the form of a packet called ECM included in the scrambled bit stream, which packet is different from the pakcet of data. Further, the work key KW is encrypted by using the master key KM and transmitted separately from program. The master key KM varies from viewer to viewer, and is distributed to a receiver (data receiving-side apparatus) in advance by using a physical medium such as an IC card.

[0016]

Assuming that each master key varying from receiver to receiver, i.e., from viewer to viewer, is KMm, one work key KM is encrypted by using each of the master keys KMm. The encryped work key KWm is transmitted in the form of a packet called EMM included in the scrambled bit stream SB, which packet is also different from packet for the program.

[0017]

The receiver receives the encrypted work key KWm corresponding to the receiver, decrypts this by using the corresponding master key KMm, and holds the corresponding work key KW in the receiver. The receiver receives the scrambled data to be broadcast in real time and the scramble key Ksn, initially decrypts the encrypted scramble key Ksn by using the work key KW held in the receiver, and then the descrambler 92 performs the descrambling process for descrambling the Pay Load 102 of the scrambled bit stream

SB by using the decrypted scramble key Ksn to produce the descrambled bit stream DB, and the separation means 93 separates the compressed audio data EDau and the compressed video data EDvi from the descrambled bit stream DB.

[0018]

Thereafter, the separated compressed audio data EDau and compressed video data EDvi are decompressed by the audio decoder 94 and the video decoder 95, respectively, to produce reproduced audio data RDau and reproduced video data RDvi, respectively.

[0019]

[Problems to be Solved by the Invention]

Using the above construction, however, the following problem arises.

Briefly stated, in a coding scheme according to MPEG4 which is currently standardized as an international standard for an image compression technique, an image signal corresponding to a scene (image corresponding to a frame) is divided into image signals respectively corresponding to a plurality of objects composing the scene, and the image signals are compressed object by object.

[0020]

On the other hand, in a coding scheme according to MPEG2 which has been already standardized, one video object composes one scene. When an audio object is handled as a

scene object, it is assumed that two objects of video object and audio object compose the scene, and then considering that the audio accompanies the image and the scene is reproduced by reusing the image corresponding to the scene, the scene is taken as being composed of one video object.

[0021]

In the coding scheme according to MPEG4, the image signal corresponding to the scene is coded for each of objects composing the scene, and in a decoding scheme according to MPEG4, coded data of respective objects is decoded for each object, and therefore it is necessary to manage a copyright for each of the objects composing the scene instead of managing it for the whole scene. That is, some of the objects composing the scene do not require protection of their copyrights, and may be copied, and then object-based copyright management is required.

[0022]

For example, when the plurality of objects composing the scene includes at least one object requiring protection of its copyright, like data handled in MPEG2 coding scheme, object data corresponding to all the objects composing the scene could be scrambled. In this case, however, respective object data are descrambled only by one-decryption of the object data corresponding to all the objects. Further, since the object data is descrambled and then the object data

corresponding to the respective objects composing the scene is individually separatable, a target object having a copyright to be protected can be extracted from the scene and it is easy to use the target object as one of a plurality of objects composing another scene.

[0023]

If the object having the copyright to be protected is illegally used, since it is difficult to prove this illegal usage, in the data transmission/receiving system according to MPEG4, the copyright might be more often violated.

[0024]

Thus, in the method in which the object data corresponding to all the objects composing the scene including the objects having copyrights to be protected are scrambled, in the data transmission/receiving system according to MPEG4, the unauthorized usage of the objects having copyrights to be protected is not prevented satisfactorily.

[0025]

The present invention is directed to solving the above-described problem, and it is an object of the present invention to provide a data processing method and a data processing apparatus as well as a data storage medium which are capable of scrambling only the objects having copyrights to be protected, among a plurality of objects composing a

scene, and is capable of satisfactorily preventing unauthorized usage of the objects having copyrights to be protected, for example, in a data transmission/receiving system according to MPEG4.

[0026]

It is another object of the present invention to provide a data processing method and a data processing apparatus which can prevent the unauthorized copying of objects which require protection of their copyrights among the plurality of objects composing the scene.

[0027]

[Measures to Solve the Problems]

A data processing method according to the present invention (Claim 1) is a data processing method for storing or transmitting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, wherein at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of objects are encrypted; and the respective object data and the scene description data are then stored or transmitted.

[0028]

According to the present invention (Claim 2), in the

data processing method of Claim 1, encryption identifiers each indicating whether or not object data corresponding to any object of the plurality of objects has been encrypted is included in the scene description data, and stored or transmitted.

[0029]

According to the present invention (Claim 3), in the data processing method of Claim 1, information required for encryption is included in the scene description data, and stored or transmitted.

[0030]

According to the present invention (Claim 4), in the data processing method of Claim 1, the scene description data is not encrypted and only object data corresponding to the objects to-be-protected is encrypted, and these data are stored or transmitted.

[0031]

According to the present invention (Claim 5), in the data processing method of Claim 1, in encrypting a plurality of object data when a plurality of objects are objects to-be-protected, a plurality of information of different types, which correspond to the respective object data, are used as information required for the encryption.

[0032]

According to the present invention (Claim 6), in the

data processing method of Claim 1, in the encryption process, a type of information required for the encryption is changed with elapse of time.

[0033]

A data processing apparatus according to the present invention (Claim 7) is a data processing apparatus for storing or transmitting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, which apparatus comprises: a plurality of data compression means respectively provided for the objects, for compressing respective object data; multiplexing means for multiplexing the scene description data and the compressed object data output from the data compression means respectively as individual streams and outputting a multiplexed bit stream; and encryption means for performing encryption for encrypting individual streams in the multiplexed bit stream which correspond to the objects to-be-protected having copyrights to be protected, to produce an encrypted bit stream, wherein the encrypted bit stream is output to the data storage medium or the data transmission medium.

[0034]

A data processing method according to the present

invention (Claim 8) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, wherein reproduction including decryption of the encrypted data and display of respective object data is performed on the encrypted data depending on whether or not the scene description data and the respective object data have been encrypted.

[0035]

A data processing apparatus according to the present invention (Claim 9) is a data processing apparatus which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data

respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, which apparatus comprises: decryption means for performing decryption for decrypting encrypted scene description data or object data according to a first control signal, to produce decrypted data; display means for displaying the scene based on the decrypted data according to a second control signal; and control means for controlling said decryption means and said display means by using the first and the second control signals so that reproduction including decryption of the encrypted data and display of respective object data is performed depending on whether or not the scene description data and the respective object data have been encrypted, when the encrypted data are received.

[0036]

A data storage medium according to the present invention (Claim 10) is a data storage medium which contains a data processing program for making a computer perform data processing for a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, wherein said data processing

program makes a computer perform: a process of encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of objects; and a process of storing or transmitting the respective object data and the scene description data after the above process.

[0037]

A data storage medium according to the present invention (Claim 11) is a data storage medium for storing digital data used for reproducing a scene, wherein said digital data includes a plurality of object data respectively corresponding to a plurality of objects which compose the scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, and is obtained by encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected.

[0038]

A data processing method according to the present invention (Claim 12) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by performing encryption for encrypting at least object data corresponding to objects to-be-protected having

copyrights to be protected among a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data and scene description data which describes how the plurality of objects compose the scene, wherein only when reproduction-ready state where encrypted object data corresponding to the objects to-be-protected is reproducible is detected, reproduction of all the object data including decryption of the object data corresponding to objects to-be-protected and display of the respective object data is performed.

[0039]

A data processing method according to the present invention (Claim 13) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data and by performing encryption for encrypting at least compressed object data corresponding to objects to-be-protected having copyrights to be protected among the compressed object data and scene description data which describes how the plurality of objects compose the scene,

wherein only when reproduction-ready state where encrypted object data corresponding to the objects to-be-protected is reproducible is detected, reproduction of all the object data including decryption of the object data corresponding to objects to-be-protected, and decompression and display of the respective object data is performed.

[0040]

According to the present invention (Claim 14), in the data processing method of Claim 13, the reproduction-ready state is a state where all the encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through a transmission medium.

[0041]

According to the present invention (Claim 15), in the data processing method of Claim 13, the reproduction-ready state is a state where the scene description data has been read from the storage medium or received through the transmission medium as well as a condition that all the encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through the transmission medium.

[0042]

According to the present invention (Claim 16), in the data processing method of Claim 13, the reproduction-ready

state is a state where the scene description data has been read from the storage medium or received through the transmission medium as well as a condition that all the object data including encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through the transmission medium.

[0043]

According to the present invention (Claim 17), in the data processing method of Claim 13, the reproduction-ready state is a state where the scene description data and all the object data which compose the scene have been read from the storage medium or received through the transmission medium.

[0044]

A data processing method according to the present invention (Claim 18) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of

compressed object data and scene description data which describes how the plurality of objects compose the scene, wherein in a decompression process of decompressing all compressed object data obtained by performing decryption for decrypting the encrypted data to produce restored object data, all the restored object data corresponding to objects are written onto reference memories and read from the reference memories; and all the restored object data are subjected to secondary encryption when it is written onto the memories and the read restored object data is subjected to decryption for decrypting the secondary encryption when it is read from the memories.

[0045]

A data processing method according to the present invention (Claim 19) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of compressed object data and scene description data which

describes how the plurality of objects compose the scene, wherein in a decompression process of decompressing all compressed object data obtained by performing decryption for decrypting the encrypted data to produce restored object data, the restored object data corresponding to the respective objects is written onto reference memories corresponding to the respective objects and read from the corresponding reference memories as required; and the restored object data is subjected to secondary encryption when it is written onto the memories and the read restored object data is subjected to decryption for decrypting the secondary encryption when it is read from the memories, the secondary encryption and the decryption being performed independently for each memory.

[0046]

A data processing apparatus according to the present invention (Claim 20) is a data processing apparatus which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected

having copyrights to be protected among the compressed object data and scene description data which describes how the plurality of objects compose the scene, which apparatus comprises: decryption means for performing decryption for decrypting the encrypted data to produce decrypted data; a plurality of data decompression means respectively provided for the objects, for decompressing compressed object data of the corresponding object included in the decrypted data, to produce decompressed object data; and a plurality of memories respectively provided for the objects, for storing decompressed object data of corresponding object, wherein each of said plurality of data decompression means includes an encryption unit for subjecting the decompressed object data to secondary encryption when the decompressed object data is output to the corresponding memory, and a decryption unit for performing decryption for decrypting the secondary encryption on the decompressed object data read from the memory.

[0047]

A data processing method according to the present invention (Claim 21) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data including display of an image data, the encrypted data being obtained by performing

encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data and scene description data which describes how the plurality of objects compose the scene, wherein the individual display of image data corresponding to objects to-be-protected having copyrights to be protected is limited.

[0048]

A data processing method according to the present invention (Claim 22) is a data processing method which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data including display of an image data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and by performing encryption for encrypting at least object data corresponding to objects to-be-protected having copyrights to be protected among the compressed object data and scene description data which describes how the plurality of objects compose the scene, wherein the image data corresponding to objects to-be-protected having copyrights to be protected is

displayed only when the compressed object data corresponding to all objects which compose the scene are decompressed.

[0049]

[Embodiments]

Embodiment 1.

Figure 1 is a block diagram for explaining a structure of a data processing apparatus according to a first embodiment of the present invention.

A data processing apparatus 1001 of the first embodiment corresponds to a data transmission-side apparatus, which is adapted to code an image signal corresponding to one frame image (scene) by a coding scheme according to MPEG4, and output the resulting signal, and includes a plurality of object compression means, provided for each of a plurality of objects composing the scene, for compressing object data corresponding to the respective objects, and scene description output means 10 for generating scene description data Dsd which describes how the respective objects compose the scene based on the image signal Dg corresponding to the scene.

[0050]

Figure 2(a) shows the scene and figure 2(b) shows its hierarchical structure, and here the scene is composed of 6 objects, i.e., 1st to 6th objects 21-26. As the above-described object compression means, the data

processing apparatus 1001 includes 1st to 6th object compression means 11 to 16 for compressing object data Do1-Do6 corresponding to the 1st to 6th objects, and outputting compressed object data EDo1-EDo6, respectively. In figure 1, the object 1 compression means 11 corresponds to a 1st object compression means, the object 2 compression means 12 corresponds to a 2nd object compression means, and the object 6 compression means 16 corresponds to a 6th object compression means.

[0051]

The data processing apparatus 1001 further includes a multiplexing means 17 for multiplexing, on the basis of the control signal, the compressed object data EDo1 to EDo6 outputted from the compression means 11 to 16 respectively and the scene description data Dsd such that the respective data are divided into packets each having a fixed size, and outputting the multiplexed bit stream MB, and a scrambling means 18a for scrambling the compressed object data corresponding to the objects to-be-protected having copyrights to be protected, which is included in the multiplexed bit stream MB, on the basis of the control signal, and outputting the scrambled bit stream SB to a transmission medium 19a or recording medium 19b, and a CPU (Central Processing Unit) 18b for outputting the respective control signals. Here, the copyright protection device 18 is

constructed by the scrambling means 18a and CPU 18b.

[0052]

As complementary explanation of the scene 20 shown in figure 2, the scene 20 corresponding to the image of one frame is shown in figure 2(a), and the objects 21-26 composing the scene 20 is grouped such that each of them belongs to one of three layers L1-L3 as shown in figure 2(b). Specifically, the video object 21 as a background image and an audio object 22 belong to an upper-most first layer L1, the video object 23 as a foreground image and the character object 26 belong to a second layer L2 just below the upper-most first layer L1, and the two video objects 24 and 25 associated with the video object 23 as the foreground image belong to a third layer L3 just below the second layer L2.

[0053]

Then, operation will be described.

In the coding scheme according to MPEG4, when transmitting the image data Dg corresponding to the scene (image corresponding to one frame and the like) 20, the image data Dg is divided into image data respectively corresponding to the objects composing the scene as shown in figure 2 and the video data (object data) Do1, Do2, ..., Do6 corresponding to the respective objects is compressed object by object.

[0054]

More specifically, in the data processing apparatus

1001 at the data transmission end, the corresponding object compression means 11, 12, ... 16 compress the object data Do1, Do2, ..., Do6 (specifically, video data, audio data, character data) corresponding to the objects 21-26 composing the scene 20, object by object, respectively, and output the compressed data as compressed object data EDo1, EDo2,..., EDo6.

[0055]

Then, in the data processing apparatus 1001 at the transmission end, the scene description output means 10 generates the scene description data Dsd which describes how the respective objects 21-26 compose the scene 20, based on the image signal Dg corresponding to the scene 20. The scene description data Dsd informs the data processing apparatus at data receiving end of the number of the objects composing the scene 20, display positions and display timings.

[0056]

When the compressed object data EDo1, EDo2, ..., EDo6, and the scene description data Dsd are input to the multiplexing means 17, the multiplexing means 17 multiplexes these data such that they have an optimum format for the transmission line (transmission medium) 19a or the storage medium 19b, and outputs the multiplexed bit stream MB.

[0057]

Figure 3(a) shows an example of the multiplexed bit

stream MB. In general, in the multiplexed bit stream MB, the scene description data Dsd is placed at the head thereof, and subsequent to the data Dsd, the respective compressed object data EDo1-EDo5 of the respective objects 21-25 are multiplexed.

[0058]

Here, since the respective video objects are moving pictures and therefore the bit stream of the compressed object data is longer one, in the multiplexed bit stream MB, the compressed object data (hereinafter also referred to as stream) of the respective objects are divided into packets each having a certain size and the packets corresponding to the respective streams are repeatedly placed. As the packet size, while the optimum size is selected according to the transmission medium or storage medium, the packet sizes of all the objects may be fixed, or the packet sizes may vary object by object. Moreover, the packet size may vary with elapse of time.

[0059]

Here, since a bit stream of the compressed object data EDo6 of the character object 26 is shorter one, this is inserted into the scene description data Dsd in the multiplexed bit stream MB.

[0060]

Further, when the multiplexed bit stream MB is input

to the scrambling means 16, the multiplexed bit stream MB is selectively scrambled object by object according to the control signal from the CPU 17 by the scrambling means 16, and the scrambled bit stream SB is output to the transmission medium 19a or the storage medium 19b. Here, the scene description data Dsd and the compressed object data EDo1, EDo3, EDo4, and EDo5 of the video objects are scrambled differently, and the compressed object data EDo2 corresnponding to the audio object is not scrambled.

[0061]

In this case, audio object 22 can be copied and duplicated after reproduced.

[0062]

Figure 3(b) shows an example of the scrambled bit stream SB, and it is known from figure 3(b) that the scene description data Dsd, the compressed object data EDo1, and the compressed object data EDo5 have been scrambled differently.

[0063]

That is, in the conventional example, a target stream to-be-scrambled is one, and therefore scrambling is controlled indiscriminately so that all or none of the objects composing the scene are scrambled. On the other hand, in this first embodiment, since scrambling of the compressed object data is selectively controlled object by object, commonly used video data or audio data as object which can

be copied are distinguishable from objects which require protection of their copyrights, and hence, protection by scrambling is not conducted for them.

[0064]

Figure 4 is an explanatory view illustrating an example of the scene description data according to MPEG4. The scene description according to MPEG4 (description indicating how respective objects compose the scene) comprises scene descriptor SD and object descriptors OD1-OD5 as descriptors, and the scene descriptor SD represents the hierarchical structure of the scene 20 shown in figure 2(b).

[0065]

That is, according to the scene descriptor SD, 2D object A1 shows that the first layer L1 includes the video object 21 and the audio object 22 and the second layer L2 represented by 2D object A2 exists. The 2D object A2 shows that the second layer L2 includes the text object 26 and the video object 23, and the third layer L3 represented by 2D object A3 exists. Further, the 2D object A3 shows that the third layer L3 includes the video objects 24 and 25.

[0066]

The scene descriptor SD also includes (an object descriptor 1)OD1 to (an object descriptor 5)OD5 which correspond to the objects 21-26, respectively.

[0067]

For example, the object descriptor 1 shows that an object number and a stream type of the corresponding object 21 is "1" and MPEG4 video, respectively, and corresponding access right information is "copying unauthorized", and the like. The object descriptor 2 shows that an object number and a stream type of the corresponding object 22 is "2" and MPEG4 audio, respectively, and corresponding access right information is "copying authorized", and the like. Each of the other object descriptors 3-5 also shows the object number, the stream type, the access right information and the like, as shown in figures 4. The object number is used for identifying the stream corresponding to each object included in the multiplexed bit stream MB.

[0068]

Since, in this first embodiment, the access right information is added to the respective object descriptors, it is not necessary for the decoding apparatus at the receiving end to directly check the scrambled bit stream SB to determine whether a stream corresponding to any object is scrambled or not, and in addition, it is possible+ to facilitate the operation for extracting only the stream of the object which can be copied from the scrambled bit stream SB.

[0069]

Subsequently, scrambling performed by the CPU 18 of the

data processing apparatus 1001 will be described with reference to figure 5.

Flowchart shown in figure 5 shows that a scramble control with respect to the stream of the respective object is performed. Scrambling of the first embodiment uses the same scheme as that of the conventional example. However, the scrambling of the first embodiment is different from the scrambling performed by the conventional data processing apparatus in that since a plurality of the objects composing the scene exist, scramble keys Ks as many as objects to-be-protected having copyrights to be protected are generated, and the streams (compressed object data) of the objects to-be-protected are scrambled by using corresponding scramble keys.

[0070]

That is, when the work key KW is input to the CPU 18a in step 501, the work key KW is encrypted by using the master key KMm and outputted in the form of EMM packet in step 502. Then, the CPU 18a generates the scramble keys Ks0 and Ks1 in Step 503, and then the scramble key Ks0 is encrypted by using the work key KW and outputted in the form of ECM packet in step 504.

[0071]

Then, the scene descriptor and the object descriptors are input to the CPU 18b in step 505 and then the protection

flag is set as access right information for each of the object descriptors object by object in step 506. Specifically, the protection flag is set for each of the object identifiers of objects to-be-protected having copyrights to be protected, and the corresponding access right information indicates that copying is unauthorized (prohibited), while the protection flag is not set for the object identifier of the object which does not require protection of its copyright, and the corresponding access right information indicates that copying is authorized (allowed).

[0072]

Then, the scramble key Ks1 is encrypted by using the scramble key Ks0 and is added to the header part of the scene description data in step 507. Further, the scene description data is encrypted by using the scramble key Ks0 and outputted in step 508.

[0073]

Thereafter, counts n and n' are set to "1" in step 509.

The count n corresponds to the object number of one of the plurality of objects composing the scene, and encryption process of encrypting the object data of the object to-be-protected for each object data by CPU 18b is performed in order of the object number. Also, the count n' corresponds to the number of times of generation of the scramble keys, each of which is generated every time the

object to-be-protected is encrypted. Hence, object data n is the object number n, and the scramble key Ksn' is generated in n'-th scrambling.

[0074]

Subsequently, the packet data is input to the CPU 18b in Step 510, and thereafter it is decided whether or not the input packet data corresponds to a new object in step 511, and when it is decided that it is not a new object, it is decided whether or not this packet data corresponds to the object having a copyright to be protected in step 512. When it is decided that this packet data corresponds to an object having a copyright to be protected, the object data n is encrypted by using the scramble key Ksn', and the encrypted object data is outputted. Then, it is decided whether or not specified time has elapsed after scrambling starts in step 520. On the other hand, when it is decided that the packet data does not correspond to an object to-be-protected in the step 512, it is immediately decided whether or not specified time has elapsed in step 520.

[0075]

When it is decided that the packet data corresponds to a new object in the Step 511, it is further decided whether or not the packet data corresponds to the object having a copyright to be protected in step 514. When it is decided that the packet data corresponds to an object to-be-protected,

a scramble key Ks(n'+ 1) is generated in Step 515, and the scramble key Ks(n'+ 1) is encrypted by using the scramble key Ksn' and added to a header of object data n in step 516. Then, the object data n is encrypted by using scramble key Ksn' and encrypted object data is outputted in step 517.

[0076]

Thereby, when the scrambled object data corresponding to a single object is taken out of the scrambled bit stream, this scrambled object data cannot be descrambled.

[0077]

To be specific, in order to descramble the object 4, a scramble key for the object 4 is necessary. However, this scramble key is included in the stream of the object 3. The scramble key for object 4 included in the header of the stream of object 3 has been encrypted by using the scramble key of the object 3, and therefore a scramble key for object 3 becomes necessary. That is, to descramble the object n, the streams of an object n and all the following objects are necessary. Thereby, without all the objects having copyrights protected, which have been transmitted, the object cannot be descrambled and this prevents these objects from being extracted individually. The scramble key is updated at regular time intervals for security like the conventional example. Then, the scramble key is updated at intervals of at least time required for scrambling the scene (an image corresponding

to one frame) as a minimum unit.

The counts n and n' are incremented in step 518, and then it is decided whether or not specified time has elapsed in the step 520.

[0078]

On the other hand, when it is decided that input packet data does not correspond to an object to-be-protected in the Step S514, the counts n and n' are incremented immediately in the step 519, and it is decided whether or not specified time has elapsed in the step 520.

[0079]

When it is decided that the specified time has elapsed in the step 520, the scramble keys Ks0 and Ks1 are updated in step S521, and then the Steps 504-520 are performed again. When it is decided that the specified time has not elapsed in the step 520, it is decided whether or not the processing of all the packet data has been completed in step 522. When it is decided that the processing has not been completed, Steps 510-522 are performed again, and when it is decided that the processing has been completed, scrambling is ended.

[0080]

Thus, in the first embodiment, the object data EDo1, EDo3-EDo6 corresponding to the objects to-be-protected having copyrights to be protected, among the plurality of objects composing the scene, are encrypted by using

predetermined encryption keys, respectively, and then the respective object data EDo1-EDo6 and the scene description data Dsd are recorded or transmitted. Therefore, the object data is encrypted selectively for the objects to-be-protected having copyrights to be protected.

[0081]

In addition, since the scene description data includes the flags for respective objects, each indicating whether or not a copyright is to be protected, at a data reading end or a data receiving end, it is decided whether or not decryption(descrambling) for the respective object data is necessary before it is actually received, whereby simplified and high-speed reproduction of the object data is achieved.

[0082]

Further, the predetermined encryption key for the encryption is included in the scene description data, and recorded or transmitted. Hence, the encryption key as well as the encrypted object data is transmitted to the data receiving end. For this reason, at the data receiving end, it is not necessary to previously hold the encryption keys. For example, if the encryption process at the data recording end or the transmission end is that of high encryption intensity using many encryption keys, the encryption keys to-be-held at the data reading end or the data receiving end are not increased.

[0083]

Still further, when plural objects are to be protected and the plural object data are encrypted, plural different encryption keys for the respective plural object data are used as the predetermined encryption keys, and thereby the encrypted object data is difficult to decrypt, and as a result the encryption process provides robust protection of the individual objects to-be-protected.

[0084]

Moreover, in the encryption process, the type of the encryption key to be used as the predetermined encryption key is changed with elapse of time, and thereby the encrypted object data is difficult to decrypt and as a result the encryption process provides robust protection of the objects to-be-protected.

[0085]

While in the first embodiment the scene description according to MPEG4 has been discussed as an example, the scene description is not restricted thereto. Any descriptor according to a coding scheme according to HTML, JAVA, or MHEG may be used so long as it represents attribute of an object.

[0086]

While the scene description is also scrambled in Step 508 as shown in figure 5, since the scene description itself includes no object data, the scene description may not be

scrambled. Also in this case, copyrights of the object can be protected.

[0087]

While in the first embodiment the scramble key is added to the header of the scene description data, no scramble key is inserted into the scene description data and the scramble keys may be added to only the object data.

[0088]

While in the first embodiment the scene description data includes the flags for the respective objects, each indicating whether or not the copyright is to be protected, the scramble keys may be unencrypted or encrypted and then added to the object descriptors of the scene description when security of the scene description data itself can be maintained.

[0089]

Embodiment 2.

Figure 6 is a diagram for explaining a data processing apparatus according to a second embodiment of the present invention and showing flow of an encryption process performed by the data processing apparatus at the data transmission end.

[0090]

The data processing apparatus of the second embodiment differs from the data processing apparatus 1001 of the first

embodiment in the details of the scrambling process, i.e., only operation of the CPU 18b for controlling the scrambling means 18a.

[0091]

Hereinafter, a description will be made to explain the scrambling process for the multiplexed bit stream MB performed by the data processing apparatus of the second embodiment.

When the work key KW is input to the CPU 18b in step 601, the work key KW is encrypted by using the master key KMm and output in the form of the EMM packet in step 602.

[0092]

Subsequently, when the scene descriptor and object descriptor are input to the CPU 18b in Step 603, the number of objects having copyrights to be protected "n" is set in step 604.

[0093]

Then, differently from the first embodiment, the scramble key Ksb longer than the scramble key of the first embodiment and scramble key Ksa of a normal length are generated in step 605, and the scramble key Ksa is encrypted by using the work key KW, and outputted in the form of ECM packet in step 606. Then, the scramble key Ksb is encrypted by using the scramble key Ksa and the encrypted scramble key Ksb is divided into n divided parts in step 607. Here, the

encrypted scramble key Ksb is bit-divided, that is, divided into a plurality of scramble keys in units of bits. To be specific, when dividing the encrypted scramble key into 3 divided parts, for example, the scramble key "1001000111" is divided into scramble key "100", scramble key "10001", and scramble key "11".

[0094]

Thereafter, when the packet data is input to the CPU 18b in step 608, it is decided whether or not the packet data corresponds to the object having a copyright to be protected in step 609. When it is decided that the packet data corresponds to the object to-be-protected having a copyright to be protected, the divided scramble keys Ksb are inserted into the user data regions or header regions of the stream (compressed object data) of the objects to-be-protected respectively in step 610. Note that the user data regions or the header regions are unscrambled.

[0095]

The stream (object data) n of the object to-be-protected is scrambled by using the scramble key Ksb in Step 611. Then, it is decided whether or not processing for all the packet data is completed in step S612.

[0096]

On the other hand, when it is decided that the input packet data does not correspond to the object to-be-protected

in the step 609, it is immediately decided whether or not processing for all the packet data is completed in Step S612.

[0097]

When it is decided that processing for all the packet data is not completed in the step 612, it is decided whether or not specified time has elapsed after scrambling starts in step 615.

[0098]

When it is decided that the specified time has elapsed in the step 612, the scramble keys Ksa and Ksb are updated in step 614, and when it is decided that the specified time has not elapsed, the Steps 606-615 are performed again without updating the scramble keys in the Step 614.

[0099]

Thus, in the second embodiment, the scramble key Ksb for scrambling all the objects to-be-protected is encrypted by using the scramble key Ksa, and thereafter the resulting encrypted scramble key Ksb is divided into the key parts corresponding to the number of the objects to-be-protected, and further the divided scramble keys Ksb are inserted into the unscrambled parts of the stream of the respective objects to-be-protected, and then the streams of the respective objects to-be-protected are scrambled by using the scramble key Ksb and output. Therefore, the scramble key Ksb cannot be reproduced unless the streams of all the objects to-

be-protected are extracted. In other words, if only a stream of an object to-be-protected are extracted, it cannot be reproduced and this provides robust protection against unauthorized copying.

[0100]

In this second embodiment, when the scramble key Ksb is divided by the number of objects "n", the scramble key Ksb is bit-divided. However, the method for dividing the scramble keys is not restricted thereto, and any method, such as a method in which the scramble key is bit-divided such that the divided key parts have different bit length or a method in which a specified bit is changed, may be used as long as the scramble key Ksb cannot be reproduced without all the objects to-be-protected in the method.

[0101]

Further, while it is explained that the CPU 18b operates differently in the first and second embodiments, the scrambling processes by the CPU 18b are not restricted thereto. Any scrambling process performed by the CPU 18b can be employed as long as the decoding cannot be performed without at least the objects to-be-protected having a copyright to be protected, which compose the scene, or a single encrypted object, if extracted, cannot be decrypted.

[0102]

The encryption process of the second embodiment, which

is different from that of the first embodiment, has an advantage that the stream of the objects to-be-protected are encrypted simply and further the descrambling is possible only when all the objects have been extracted, while it has a drawback that if the portions in the stream into which the scramble key Ksb are inserted are extracted, then descrambling is performed with ease. Accordingly, it becomes necessary to select one of the encryption processes of the first embodiment and the encryption processes of the second embodiment as an optimum encryption process according to system configuration.

[0103]

Embodiment 3.

Figures 7 are block diagrams for explaining a data processing apparatus configuration according to a third embodiment of the present invention.

A data processing apparatus 1003 of the third embodiment corresponds to a data receiving-side apparatus adapted to receive the bit stream SB obtained by performing coding on the image signal corresponding to one frame image (scene) by the coding scheme according to MPEG4, and the like, and reproduce the bit stream. Here, the bit stream SB is scrambled by a data transmission-side apparatus having a similar construction to that of the data processing apparatus of the first embodiment.

[0104]

The data processing apparatus 1003 includes descrambling means 71 for descrambling the input scrambled bit stream SB according to the control signal to produce a descrambled bit stream DB, and a separation means 73 for separating the scene description data and the object data of respective objects from the descrambled bit stream DB.

[0105]

The data processing apparatus 1003 further includes a plurality of object decompression means provided for the respective objects, for decompressing corresponding compressed object data according to control signals, and scene description reproduction means 77 which receives the scene description data separated from the descrambled bit stream, processes the data necessary for scene composition and outputs the processed data.

[0106]

Here, the data processing apparatus 1003 includes a first to sixth object 1 decompression means 74, 75, ···,76 as object decompression means adapted to the data transmission-side apparatus 1001, which decompress the compressed object data EDo1 - EDo6 of a first to sixth objects 21 - 26 and output decompressed object data RDo1 - RDo6. In figure 7, the object 1 decompression means 74 corresponds to the first object decompression means, the object 2

decompression means 75 to the second object decompression means, the object 6 decompression means 76 to the sixth object decompression means.

[0107]

In MPEG coding scheme, as image data corresponding to a current frame is encoded and transmitted as difference data between image data of a previous frame and the image data of the current frame, it is necessary to store image data of a restored previous frame when decompressed object data is produced. Therefore, the data processing apparatus 1003 includes 6 reference memories, i.e., reference memories 741, 751, . . . 761, corresponding to the object decompression means 74, 75, . . ., 76, respectively.

[0108]

The data processing apparatus 1003 still further includes composition means 78 for compositing the decompressed object data EDo1-EDo6 to restore an image signal corresponding to a scene according to the reproduced scene description data, display means 79 which receives the image signal RD which has been restored by the composition means 78 and displays the image corresponding to the scene according to the control signal, and a CPU 72 for controlling the scrambling means, the respective decompression means, the scene description reproduction means, and the display means by using respective control signals. Here, the

descrambling means 71 and the CPU 72 constitute the receiving-side copyright protection device 3.

[0109]

Operation will now be described.

Figure 8 is a flowchart for explaining operation of the CPU 72 constituting the copyright protection device and showing processing in which the descrambling means 71 descrambles the input bit stream under control of the CPU 72. In other words, figure 8 shows the control operation performed by CPU 72 in descrambling and the operation performed by CPU 72 shown in figure 8 flows in the almost reversed order of the operation of the CPU 18b of the first embodiment. The scrambled bit stream SB outputted from the data processing apparatus 1001 of the first embodiment is to be input to the copyright protection device 3 included in the data processing apparatus 1003.

[0110]

When the scrambled bit stream SB is input to the copyright protection device 3, the descrambling means 71 descrambles the scrambled bit stream SB according to the control signal from the CPU 72.

[0111]

That is, initially, in step 801, the work key KW is extracted from EMM packet included in the scrambled bit stream SB and the work key KW is decrypted by using master

key KMm. Subsequently, in step 802, the scramble key Ks0 is extracted from ECM packet included in the scrambled bit stream SB, and the scramble key Ks0 is decrypted by using the work key KW.

[0112]

Then, the scene description data is input and the scene description data is decrypted by using the scramble key Ks0 in step 803. Subsequently, in step 804, the scramble key Ks1 is extracted from the scene description data and the scramble key Ks1 is decrypted by using the scramble key Ks0.

[0113]

Thereafter, in Steps 805-817, for each of the objects having a copyright to be protected, extraction of a scramble key and decryption of the scramble key, and descrambling of the object data are repeatedely performed in the order of ascending object numbers represented as the object descriptors.

[0114]

That is, the counts n and n' identical to those of the first embodiment are respectively set to "1" in step 805, and then the packet data is input to CPU 72 in step 806. Thereafter, it is decided whether or not the input packet data corresponds to a new object in step 807, and when it is decided that the packet data does not correspond to a new object, it is decided whether or not the input packet data

corresponds to the object having a copyright to be protected in step 808. When it is decided that the packet data corresponds to the object having a copyright to be protected, the object data n is decrypted by using the scramble key Ksn' to produce the restored object data. Then, it is decided whether or not processing for all the data is completed in step 817.

[0115]

When it is decided that the packet data does not correspond to the object to-be-protected in the step 808, it is immediately decided whether or not processing for all the data is completed in the step 817.

[0116]

When it is decided that the packet data corresponds to a new object in the step 807, it is further decided whether or not the packet data corresponds to the object to-be-protected having a copyright to be protected in step 810. When it is decided that the packet data corresponds to the object to-be-protected, the scramble key Ks(n' + 1) is extracted from the header of the object data n in step 810 and the decrypted scramble key Ks(n' + 1) is outputted to the descrambling means for the object (n' + 1) in step 812. Further, the object data n is descrambled by using the scramble key Ksn' and the restored object data n is output in step 813. Then, the counts n and n' are incremented by

one in step 814 and it is decided whether or not processing for all the data is completed in the step 817.

[0117]

On the other hand, when it is decided that the input packet data does not correspond to the object to-be-protected in the step 810, the count n is immediately incremented by one in step 815, and it is decided whether or not processing for all the data is completed in the step 817.

[0118]

When it is decided that descrambling process for all the object data is not completed in the step 817, it is decided whether or not the scramble key Ks0 is updated in step 816. When it is decided that the scramble key Ks0 is updated, Steps 802-817 are performed again, and when it is decided that the scramble key Ks0 is not updated, Steps 806-817 are performed again.

[0119]

Thereafter, the descrambled bit stream is separated into object data corresponding to the respective objects and scene description data by the separation means 73. Here, the compressed object data for each object such as image and audio data are decompressed by the decompression means 74, 75,...,76 of the respective objects and the resulting data are converted into displayable data (decompressed object data RD01 to RD06).

[0120]

The decompressed object data which has been restored by the respective object decompression means 74, 75, ..., 76 are composited by the composition means 78 to produce an image signal RD corresponding to a scene (frame image) and the scene is displayed on the display means 79 based on the image signal RD.

[0121]

Thus, in the third embodiment, for the encrypted data obtained by selectively encrypting the plural object data of the plural objects composing the scene and the scene description data which describes how the plural objects compose the scene, reproduction including decryption of the encrypted data and display of the respective object data, is performed, depending upon whether or not the scene description data and the respective object data have been encrypted. Therefore, decryption can be performed for the bit stream which is scrambled by using scramble keys varying object by object, in which bit stream the scramble key used for scrambling subsequent object data is inserted into the header part of the object data which is scrambled previously. Thereby, based on the scrambled bit stream output from the data processing apparatus of the first embodiment, the image signal corresponding to the scene can be reproduced.

[0122]

While in the third embodiment the display means 79 always displays the image signal output from the composition means 78, the CPU 72 may execute control so that the display means 79 displays the output from the composition means 78 only when specific conditions is satisfied.

[0123]

For example, using the construction in which the display means 79 always displays the output RD from the composition means 78, when the composition means 78 outputs a single object data, only the single object is displayed. For this reason, there may be a possibility that the scrambled bit stream which has been subjected to scrambling process is decrypted and illegally reproduced, and the stream of the object to-be-protected having a copyright to be protected is extracted from the reproduced bit stream for use.

[0124]

Then, the display means 79 is controlled by the CPU 72, and only when the CPU 79 recognizes that the specific condition is satisfied, the display means 79 may display image outputted from the composition means 78.

[0125]

Here, as the specific conditions, it can be considered that the CPU 72 confirms that all the objects composing the scene to be displayed have been descrambled as well as decompression for the object data of the objects required

and composition of the object data in the composition means 78 are completed, and the like.

[0126]

As conditions other than the conditions described above, the following are conceived.

For example, when it is detected that all the encrypted object data of the objects to-be-protected having copyrights to be protected are readable from the storage medium or receivable through the transmission medium, all the object data are reproduced.

[0127]

Further, when the scene description data has been read or received and it is detected that all the encrypted object data of the objects to-be-protected having copyrights to be protected are readable from the storage medium or receivable through the transmission medium, all the object data are reproduced.

[0128]

Moreover, when the scene description data has been read or received and it is detected that all the object data of all the objects composing the scene are readable from the storage medium or receivable through the transmission medium, all the object data are reproduced.

[0129]

Still further, when the scene description data and all

the object data composing the scene have been read from the storage medium or received through the transmission medium, all the object data are reproduced.

[0130]

Under these conditions, the display means 79 outputs only an image signal corresponding to a composite scene to a display. This makes it difficult to take out the video data of the objects to-be-protected having copyrights to be protected, which provides robust protection of the copyright in the data transmission/receiving system. To detect these conditions, the CPU 72 inquires a storage medium or a server at a transmission end of the existence/non-existence of the respective object data or the scene description data.

[0131]

Moreover, in the third embodiment, a description is given of the data receiving-side apparatus which receives the encrypted bit stream obtained by scrambling the stream parts of respective objects included in bit stream and descrambles the bit stream and reproduces the descrambled bit stream. However, in the data receiving-side apparatus adopting the coding scheme according to MPEG4 like the third embodiment, also when data access is made to the reference memory for storing restored data when decompressing the compressed data, scrambling and descrambling may be performed. This also provides robust protection of the

objects having copyrights to be protected.

[0132]

Specifically, in the data transmission system using the coding scheme according to MPEG standard, since difference data between a current frame and a previous frame is compressed and the difference data is transmitted as an image data of the current frame, it is necessary to store restored image data of the previous frame when decompressing the compressed data. Hence, the image data restored by the respective object decompression means is stored in corresponding reference memories.

[0133]

In the data receiving-side apparatus in which the reference memory is constituted by hardware, it is difficult to copy the contents in the reference memory because the apparatus needs to be reconfigured, while in the data receiving-side apparatus in which the reference memory is constituted by software, since the object data, i.e., video data corresponding to the respective objects is written into the storage on the computer, for example, the contents of the reference memory can be taken out by creating a special program.

[0134]

The object decompression means of the third embodiment may be adapted to encrypt object data and write encrypted

object data onto the reference memory, and decrypt the encrypted object data read from the reference memory.

[0135]

Figure 7(b) shows a specific structure of object decompression means 740 which performs scrambling and descrambling also when accessing the data in the reference memory.

[0136]

The object decompression means 740 comprises a decompression unit 74 for decompressing the compressed object data of the object output from the separation means 73, a scrambling unit 74b for scrambling the decompressed object data and outputting scrambled object data to a reference memory, and a descrambling unit 74c for descrambling data read from the reference memory and returning descrambled data to the decompression unit 74a.

[0137]

Though only the object 1 decompression means of the third embodiment is shown in figure 7(b), the other object decompression means have the structure identical to those shown in figure 7(b).

[0138]

The scrambling method performed when accessing the memory for the object data is not limited to the scrambling method performed for each memory for each object data. The

image signal corresponding to the scene obtained by compositing the respective object data by the use of the composition means may be collectively scrambled when temporarily stored in the memory.

[0139]

As the scrambling method, various types of methods may be employed depending upon how robust protection of copyright should be, or easiness of copying the contents of the reference memory in the system, or the like, such as a method similar to the scrambling of the first embodiment used when the bit stream is transmitted or recorded, a simplified method of the scrambling of the above method, i.e., a method which uses the scramble keys used for scrambling respective object data for the encryption process when accessing the memory, or a method which uses the scramble key Ks0 for the scene description data.

[0140]

While in the above first to third embodiments the number of objects is described as "6", the number of the objects is not limited to this. In addition, while a description is given of a multiplexing process in which the object and the scene description are multiplexed into one stream and outputted, the multiplexing process is not restricted thereto. Data which is transmitted packet by packet on the Internet, may be handled like the packet data in one

multiplexed bit stream, whereby the same effects are provided.

[0141]

Further, while in each of the above embodiments the scrambling method is described using an example of the same method as the conventional one, the scrambling method is not restricted thereto. Any scrambling which achieves the aim, such as a method using encryption stronger than that of the scrambling described in the above embodiments or a method using a generalized common encryption key or a public key, is applied to the encryption of the present invention.

[0142]

Further, a method in which an electronic water mark data or the like is superimposed on the contents (object data) itself when outputting or compressing data and from detection of the water mark data when receiving or decompressing data, it is decided whether or not such contents have the copyright which has been protected may be employed.

[0143]

While in each of the above embodiments a description is given of the case where the coding scheme according to MPEG4 is used, coding scheme in data transmission system is not restricted thereto, and any system which makes data transmission for each of plural objects composing a scene may be used regardless of the type of the data compression

according to MPEG1, MPEG, JPEG, H.261, H.263, and the like. Furthermore, the scrambling for each object of the present invention is also applied to a data transmission system which is not adapted to compress the data.

[0144]

While in each of the above embodiments the data processing apparatus includes the copyright protection device which scrambles or descrambles the bit stream independently of the data compression means or the data decompression means, the data processing apparatus is not limited to this.

[0145]

For instance, the object compression means in the data processing apparatus at the transmission end may be adapted to compress and scramble the object data simultaneously. To be specific, compressed data, which cannot be restored through a normal decompression process, is generated by scrambling data of a motion vector, scrambling a part of DCT coefficients, or inverting a part of compressed object data according to a prescribed rule, and the compressed object data of all the objects having copyrights to be protected, can be restored by decompression only when they are all present at the data receiving side. This provides the similar effects to those of each of the above embodiments.

[0146]

Furthermore, a data processing program for implementing the data processing method shown in each of the embodiments is stored in a data storage medium such as a floppy disc, whereby processing described in each of the above embodiments is performed with ease in an independent computer system.

[0147]

Figure 10 is a diagram for explaining a case where coding or decoding according to the first to sixth embodiments is performed in a computer system by using a floppy disc which contains the coding or decoding program.

[0148]

Figure 11(a) shows a front appearance and a cross-section of a floppy disc, and a floppy disc body, and figure 11(b) shows an example of a physical format of the floppy disc body.

[0149]

The floppy disc FD has such a construction thatthe floppy disc body D is stored in a floppy disc case FC, and in a surface of the floppy disc body D, plural tracks Tr are concentrically formed from outer to inner circumferences thereof, each track Tr being divided into 16 sectors Se in angle direction. Therefore, in the floppy disc FD which contains the program, data of the program is recorded in an allocated region (Sector) Se of the floppy disc body D.

[0150]

Further, figure 11(c) shows a construction for recording the program into the floppy disc FD and performing image processing using the program stored in the floppy disc FD.

[0151]

In the case of recording the program in the floppy disc FD, the data as the program is written into the floppy disc FD through the floppy disc drive FDD from the computer system Cs. Further, in the case of constructing the arbitrary shape coding apparatus or the arbitrary shape decoding apparatus in the computer system Cs by the program recorded in the floppy disc FD, the program is read from the floppy disc FD by the use of the floppy disc drive FDD and loaded into the computer system Cs.

[0152]

Further, the scrambled bit stream output from the data processing apparatus of the first embodiment may be stored in the storage medium. In this case, the storage medium in which the image signal which is copyright-protected for each object composing a scene is stored can be obtained.

[0153]

While a floppy disc is used as a data storage medium in the above description, coding or decoding with using software can be performed like that using the floppy disc also when an optical disc is used. Besides, the storage

medium is not limited to the optical disc or the floppy disc, and an IC card, a ROM cassette, and so forth, may be used so long as they can record a program therein. Also when these recording mediums are used, coding or decoding with using software can be carried out as in the case of using the floppy disc or the like.

[0154]

[Effect of the Invention]

As descried above, in a data processing method according to the present invention (Claim 1), object data corresponding to objects to-be-protected having copyrights to be protected among a plurality of objects which compose a scene are encrypted; and then the respective object data and the scene description data are stored or transmitted. Therefore, the object data is selectively encrypted so that object to-be-protected having a copyright to be protected is encrypted.

[0155]

According to the present invention (Claim 2), in the data processing method of Claim 1, encryption identifiers each indicating whether or not object data corresponding to any object of the plurality of objects has been encrypted is included in the scene description data, and stored or transmitted. Therefore, at a data reading end or a data receiving end, it is decided whether or not decryption is

necessary before the respective object data is actually received, whereby simplified and high-speed reproduction of the object data is achieved.

[0156]

According to the present invention (Claim 3), in the data processing method of Claim 1, information required for the encryption is included in the scene description data, and stored or transmitted. Therefore, information required for encryption such as an encryption key as well as encrypted object data are transmitted to the data receiving end, and thereby, at the data receiving end, it is not necessary to hold the encryption keys and the like in advance. For example, if the encryption process at the data recording end or transmission end is that of high encryption intensity using many encryption keys, the encryption keys to-be-held at the data reading end or the data receiving end are not increased.

[0157]

According to the present invention (Claim 4), in the data processing method of Claim 1, the scene description data is not encrypted and only object data corresponding to the objects to-be-protected having copyrights to be protected is encrypted, and these data are stored or transmitted. Therefore, at the data recording end or the data transmission end, only the object data corresponding to the objects

to-be-protected are efficiently encrypted, whereby simplified and high-speed encryption is achieved.

[0158]

According to the present invention (Claim 5), in the data processing method of Claim 1, in encrypting a plurality of object data when a plurality of objects are objects to be protected, a plurality of information of different types, which correspond to the respective object data, are used as information required for the encryption. Therefore, the encrypted object data is difficult to decrypt, and such encryption process provides robust protection of the individual objects to-be-protected.

[0159]

According to the present invention (Claim 6), in the data processing method of Claim 1, in the encryption process, a type of information required for the encryption is changed with elapse of time. Therefore, the encrypted object data is difficult to decrypt, and such encryption process provides robust protection of the objects to-be-protected.

[0160]

A data processing apparatus according to the present invention (claim 7) comprises: a plurality of data compression means respectively provided for a plurality of objects composing a scene, for compressing the respective object data; multiplexing means for multiplexing the scene

description data and the compressed object data output from the data compression means respectively as individual streams and outputting a multiplexed bit stream; and encryption means for performing encryption for encrypting individual streams in the multiplexed bit stream which correspond to the objects to-be-protected having copyrights to be protected, to produce an encrypted bit stream, and the apparatus outputs the encrypted bit stream to the data storage medium or the data transmission medium. Therefore, the object data is selectively encrypted so that object to-be-protected having a copyright to be protected is encrypted.

[0161]

In a data processing method according to the present invention (Claim 8), reproduction including decryption of encrypted data and display of respective object data is performed on the encrypted data obtained by selectively encrypting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and scene description data which describes how the plurality of objects compose the scene, depending on whether or not the scene description data and the respective object data have been encrypted. Therefore, at the data reading end or the receiving end, the encrypted object data or the encrypted scene description data is selectively decrypted, whereby the

encrypted data is reproduced efficiently.

[0162]

A data processing apparatus according to the present invention (Claim 9) is an apparatus which reads the encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by selectively performing encryption of a plurality of object data respectively corresponding to a plurality of objects which compose a scene and scene description data which describes how the plurality of objects compose the scene, and the apparatus comprises: decryption means for selectively performing decryption for the encrypted data to produce decrypted data, and display means for displaying the scene based on the decrypted data; and control means for controlling the decryption means and the display means so that reproduction including decryption of the encrypted data and display of respective object data is performed depending on whether or not the scene description data and the respective object data have been encrypted. Therefore, the encrypted object data or the encrypted scene description data is selectively decrypted, whereby the encrypted data is reproduced efficiently.

[0163]

According to a data storage medium of the present

invention (Claim 10), a data processing program makes a computer perform: a process of encrypting object data corresponding to objects to-be-protected having copyrights to be protected among the plurality of objects composing a scene; and then a process of storing or transmitting the respective object data and the scene description data. Therefore, selective encryption for the objects to-be-protected having copyrights to be protected among a plurality of objects, is realized by software.

[0164]

In a data storage medium according to the present invention (Claim 11), stored digital data includes a plurality of object data respectively corresponding to a plurality of objects which compose the scene and scene description data which describes how the plurality of objects compose the scene, and is obtained by encrypting object data corresponding to objects to-be-protected having copyrights to be protected. Therefore, at a data reading end, the encrypted object data or the encrypted scene description data is selectively decrypted, whereby the encrypted data is reproduced efficiently.

[0165]

In a data processing method according to the present invention (Claim 12), when encrypted data obtained by performing a predetermined encryption on a plurality of

object data respectively corresponding to a plurality of objects which compose a scene and scene description data which describes how the plurality of objects compose the scene is read from a storage medium or received through a transmission medium and reproduced, only when reproduction-ready state where encrypted object data corresponding to the objects to-be-protected having copyrights to be protected is reproducible is detected, reproduction of all the object data including decryption of the encrypted object data corresponding to objects to-be-protected and display of the respective object data is performed. Therefore, intensity of protection for object to-be-protected can be enhanced and illegal usage such as unauthorized copying of objects requiring copyrights protection becomes difficult.

[0166].

In a data processing method according to the present invention (Claim 13), when encrypted data obtained by compressing object data respectively corresponding to a plurality of objects which compose a scene and performing a predetermined encryption on the compressed object data and scene description data which describes how the plurality of objects compose the scene is read from a storage medium or received through a transmission medium and reproduced, only when reproduction-ready state where encrypted object data

corresponding to the objects to-be-protected having copyrights to be protected is reproducible is detected, reproduction of all the object data including decryption of object data corresponding to objects to-be-protected. and decompression and display of the respective object data is performed. Therefore, intensity of protection for object to-be-protected can be enhanced and illegal usage such as unauthorized copying of objects requiring copyright protection becomes difficult.

[0167]

According to the present invention (Claim 14), in the data processing method of Claim 13, the reproduction-ready state is a state where all the encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through a transmission medium. Therefore, only when object data corresponding to the objects to-be-protected are all present in the storage medium for the object data or at the transmission end, the object to-be-protected is reproduced.

[0168]

This effectively prevents illegal usage such as unauthorized copying of the objects to-be-protected.

[0169]

According to the present invention (Claim 15), in the data processing method of Claim 13, the reproduction-ready

state is a state where the scene description data has been read from the storage medium or received through the transmission medium as well as a condition that all the encrypted object data corresponding to the objects to-be-protected can be read from the storage medium or can be received through the transmission medium. Therefore, only when the object data corresponding to the objects to-be-protected is all present in the storage medium for the object data or at the transmission end, and the scene description data has been read or received, object to-be-protected is reproduced. This effectively prevents illegal usage such as unauthorized copying of the objects to-be-protected.

[0170]

According to the present invention (Claim 16), in the data processing method of Claim 13, the reproduction-ready state is a state where the scene description data has been read from the storage medium or received through the transmission medium as well as a condition that all the object data including encrypted object data can be read from the storage medium or can be received through the transmission medium. Therefore, only when the object data corresponding to the objects which compose a scene are all present in the storage medium for the object data or at the transmission end, and the scene description data has been read or received, object to-be-protected is reproduced. This more

effectively prevents illegal usage such as unauthorized copying of the objects to-be-protected.

[0171]

According to the present invention (Claim 17), in the data processing method of Claim 13, the reproduction-ready state is a state where the scene description data and all the object data which compose the scene have been read from the storage medium or received through the transmission medium. Therefore, individual reproduction of object to-be-protected among a plurality of objects composing a scene is limited, and this satisfactorily prevents illegal usage such as unauthorized copying of the objects to-be-protected.

[0172]

In a data processing method according to the present invention (Claim 18), when encrypted data obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and performing a predetermined encryption on the plurality of compressed object data and scene description data which describes how the plurality of objects compose the scene is read from a storage medium or received through a transmission medium and reproduced, in a decompression process of decompressing all compressed object data obtained by decrypting the encrypted data to produce restored object data,

all the restored object data corresponding to objects are written onto reference memories and read from the reference memories; and all the restored object data are subjected to secondary encryption when it is written onto the memories and the read restored object data is subjected to decryption for decrypting the secondary encryption when it is read from the memories. Therefore, at the data reading end or the data receiving end, the object data of the objects to-be-protected stored in the reference memories in the decompression process is prevented from being illegally utilized such as being illegally copied, thereby improving robustness of protection of the objects to-be-protected.

[0173]

In a data processing method according to the present invention (Claim 19), when encrypted data obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and performing a predetermined encryption on the plurality of compressed object data and scene description data which describes how the plurality of objects compose the scene is read from a storage medium or received through a transmission medium and reproduced, in a decompression process of decompressing all compressed object data obtained by decrypting the encrypted data to produce restored object data, the restored object data corresponding to the respective

objects are written onto reference memories corresponding to the respective objects and read from the corresponding reference memories as required; and the restored object data are subjected to secondary encryption when it is written onto the memories and the read restored object data are subjected to decryption for decrypting the secondary encryption when it is read from the memories, the secondary encryption and the decryption being performed independently for each memory. Therefore, at the data reading end or the data receiving end, the object data of the objects to-be-protected stored in the reference memories in the decompression process is prevented from being illegally utilized such as being illegally copied, for each object to-be-protected, thereby selectively improving robustness of protection of a plurality of objects to-be-protected.

[0174]

A data processing apparatus according to the present invention (Claim 20) is an apparatus which reads encrypted data from a storage medium or receives the encrypted data through a transmission medium and performs reproduction of the encrypted data, the encrypted data being obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and performing a predetermined encryption on the compressed object data and scene description data which describes how

the plurality of objects compose the scene, which apparatus comprises: decryption means for decrypting the encrypted data to produce decrypted data; a plurality of data decompression means respectively provided for the objects, for decompressing compressed object data included in the decrypted data, to produce decompressed object data; and a plurality of memories respectively provided for the objects, for storing decompressed object data of object, in which apparatus each of said plurality of data decompression means includes an encryption unit for subjecting the decompressed object data to secondary encryption when the decompressed object data is output to the corresponding memory, and a decryption unit for performing decryption for decrypting the secondary encryption on the decompressed object data read from the memory. Therefore, at the data reading end or the data receiving end, the object data of the objects to-be-protected stored in the reference memories in the decompression process is prevented from being illegally utilized such as being illegally copied, for each object to-be-protected, thereby selectively improving robustness of protection of a plurality of objects to-be-protected.

[0175]

In a data processing method according to the present invention (Claim 21), when encrypted data obtained by performing a predetermined encryption on a plurality of

object data respectively corresponding to a plurality of objects which compose a scene and scene description data which describes how the plurality of objects compose the scene is read from a storage medium or received through a transmission medium and the reproduction of encrypted data including display of image data is performed, the individual display of image data corresponding to objects to-be-protected having copyrights to be protected is limited. Therefore, this makes it difficult to illegally utilize (conduct unauthorized copying of) the objects to-be-protected.

[0176]

In a data processing method according to the present invention (Claim 22), when encrypted data obtained by compressing a plurality of object data respectively corresponding to a plurality of objects which compose a scene and by performing a predetermined encryption on the compressed object data and scene description data which describes how the plurality of objects compose the scene is read from a storage medium or received through a transmission medium and the reproduction of encrypted data including display of image data is performed, the image data corresponding to objects to-be-protected having copyrights to be protected is displayed only when the compressed object data corresponding to all objects which compose the scene

are decompressed. Therefore, this makes it difficult to illegally utilize (conduct unauthorized copying of) the objects to-be-protected.

[Brief Description of the Drawings]

[Figure 1]

Figure 1 is a block diagram for explaining a data processing apparatus according to a first embodiment of the present invention.

[Figure 2]

Figures 2 are diagrams for explaining conception of an object coding scheme according to MPEG4 performed by the data processing apparatus of the first embodiment, and showing a scene composed of a plurality of objects (figure 2(a)) and its hierarchical structure (figure 2(b)).

[Figure 3]

Figure 3(a) is a schematic diagram showing a multiplexed bit stream produced by the data processing apparatus of the first embodiment and figure 3(b) is a schematic diagram showing a scrambled bit stream which has been scrambled.

[Figure 4]

Figures 4 are diagrams for explaining an example of scene description used by the object coding scheme of the first embodiment.

[Figure 5]

Figure 5 is a diagram showing flow of scrambling

performed by a CPU of the data processing apparatus of the first embodiment.

[Figure 6]

Figure 6 is a diagram showing flow of scrambling performed by a CPU of a data processing apparatus of a second embodiment of the present invention.

[Figure 7]

Figures 7 are diagrams for explaining a data processing apparatus according to a third embodiment of the present invention, wherein figure 7(a) shows a structure of the data processing apparatus of the third embodiment and figure 7(b) shows a structure of object decompression means of a data processing apparatus according to modification of the third embodiment.

[Figure 8]

Figure 8 is a diagram showing flow of descrambling performed by a CPU of the data processing apparatus of the third embodiment.

[Figure 9]

Figure 9 is a diagram showing a data transmission/receiving system which adopts a conventional conditional access method.

[Figure 10]

Figure 10 is a diagram showing structures of packets of the multiplexed bit stream which is output from a data

transmission-side apparatus in the conventional data transmission/receiving system.

[Figure 11]

Figures 11(a) and 11(b) are diagrams for explaining a data storage medium which contains a program for implementing the data processings of each of the embodiments in a computer system and figure 11(c) is a diagram showing the computer system.

[Description of the Reference Numerals]

1,3 copyright protection device

10 scene description output means

11 object 1 compression means

12 object 2 compression means

13 object 3 compression means

14 scene description output means

15 multiplexing means

16 scrambling means

17, 72 CPU

18 transmission medium

19 storage medium

71 descrambling means

73 separation means

74, 740 object 1 decompression means

74a scrambling unit

74b descrambling unit

74c decompression unit

75 object 2 decompression means

76 object 3 decompression means

77 scene description reproduction means

78 composition means

79 display means

81 data transmission-side apparatus

82 audio encoder

83 video encoder

84 multiplexing unit

85 scrambler

91 data receiving-side apparatus

92 descrambler

93 separation unit

94 audio decoder

95 video decoder

100a packet

1000 data transmission/receiving system

1001, 1003 data processing apparatus

MB multiplexed bit stream

SB scrambled bit stream

DB descrambled bit stream

[Name of Document] Abstract

[Summary]

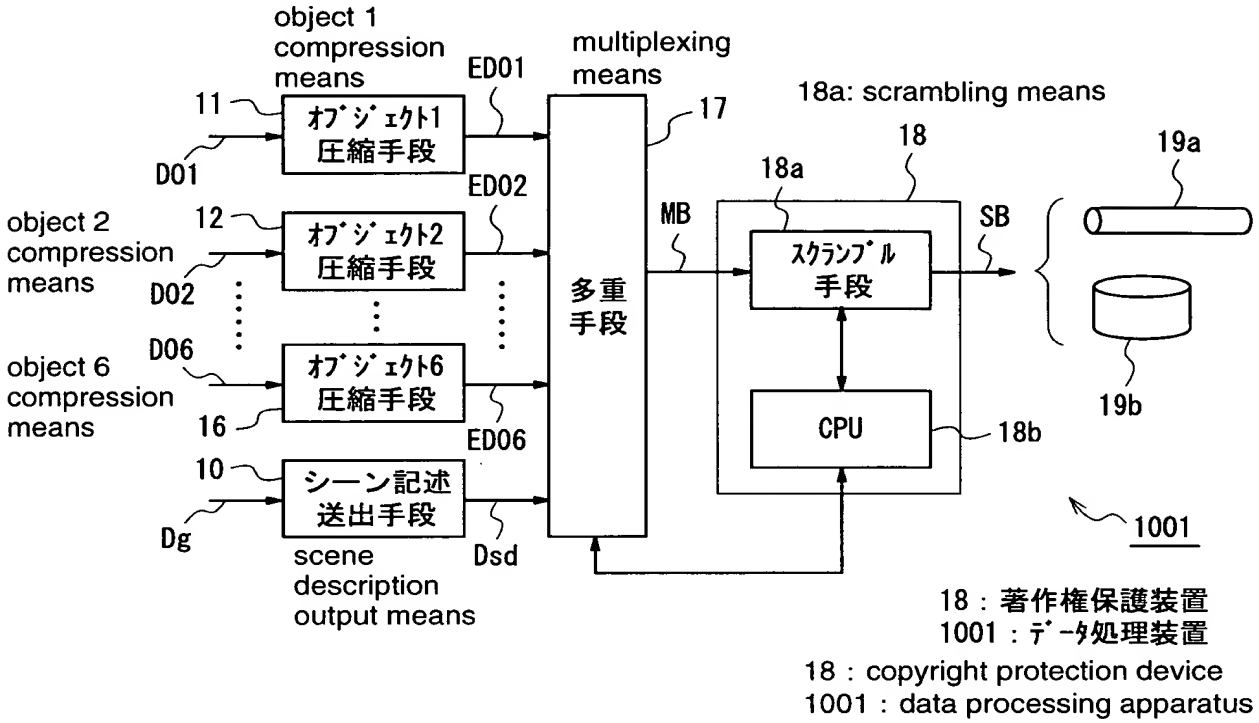
[Object] Encryption for each of object data can be selectively performed on object to-be-protected having copyright to be protected.

[Construction] There are provided a plurality of data compression means 11-13 for compressing respective object data respectively corresponding to a plurality of objects which compose a scene, multiplexing means 15 for multiplexing scene description data and compressed object data to output a multiplexed bit stream MB, and scrambling means 16 for performing encryption process for scrambling individual streams corresponding to the objects to-be-protected having copyrights to be protected in the multiplexed bit stream MB, to produce a scrambled bit stream SB, and the scrambled bit stream SB is output to a data storage medium 19 or a data transmission medium 18.

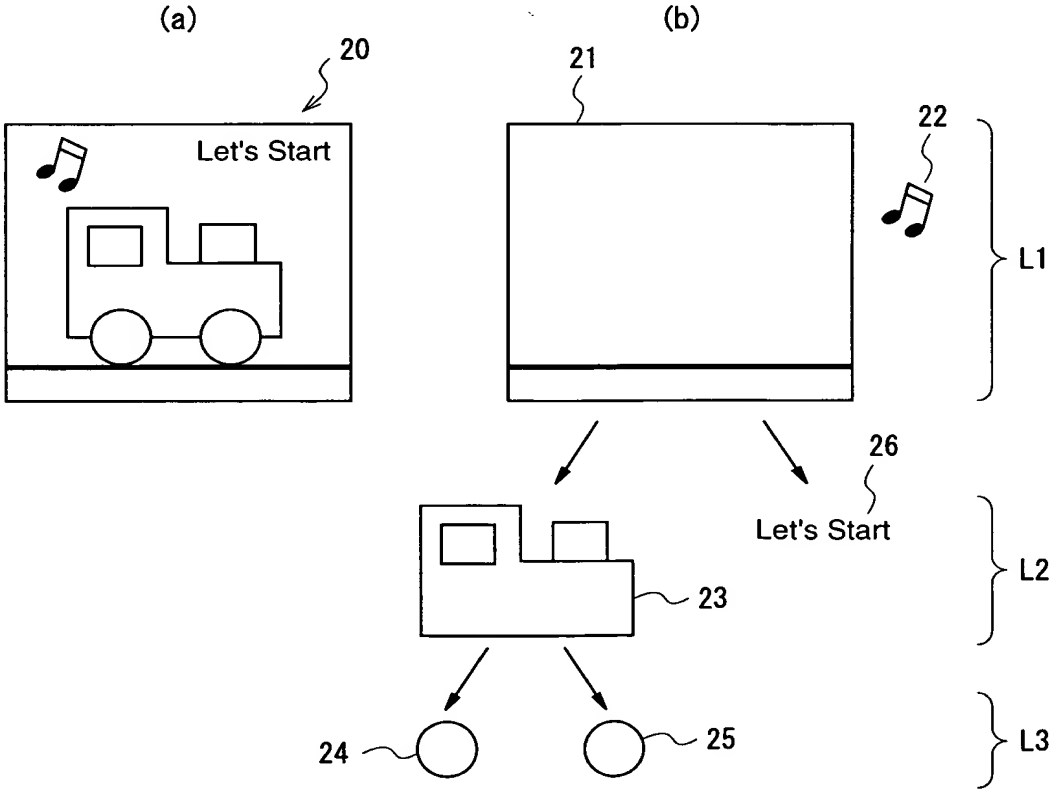
[Selected Figure] Figure 1

Name of Document
【書類名】 図 面 Drawing

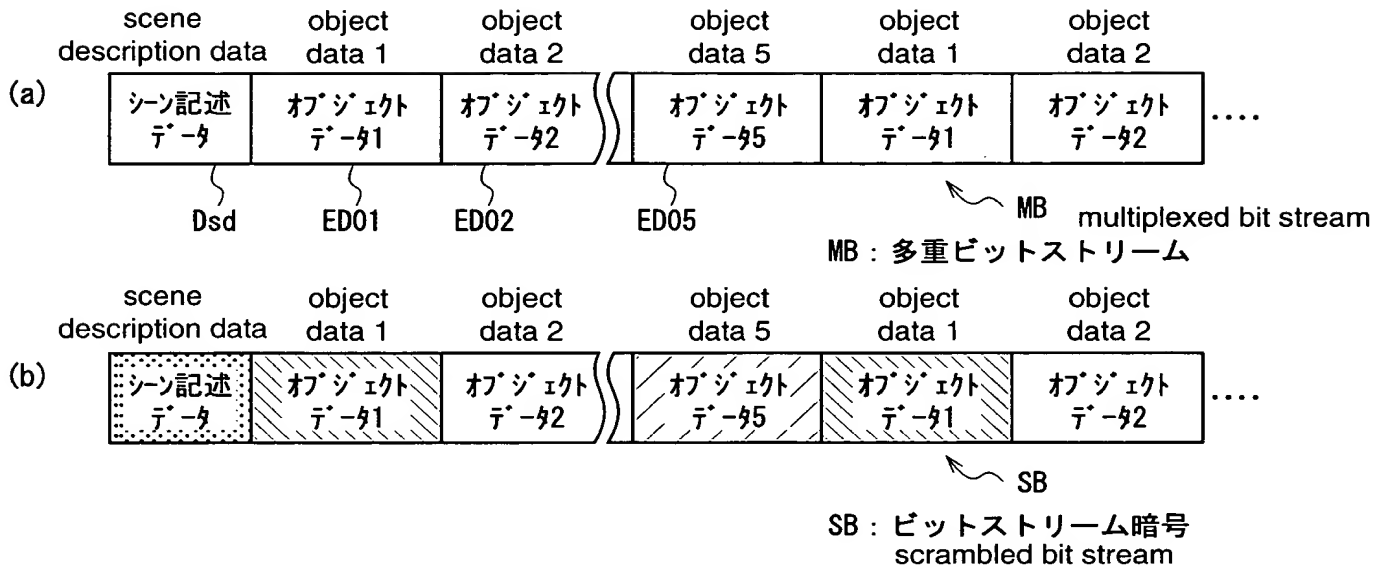
【図1】 Figure 1



【図2】 Figure 2



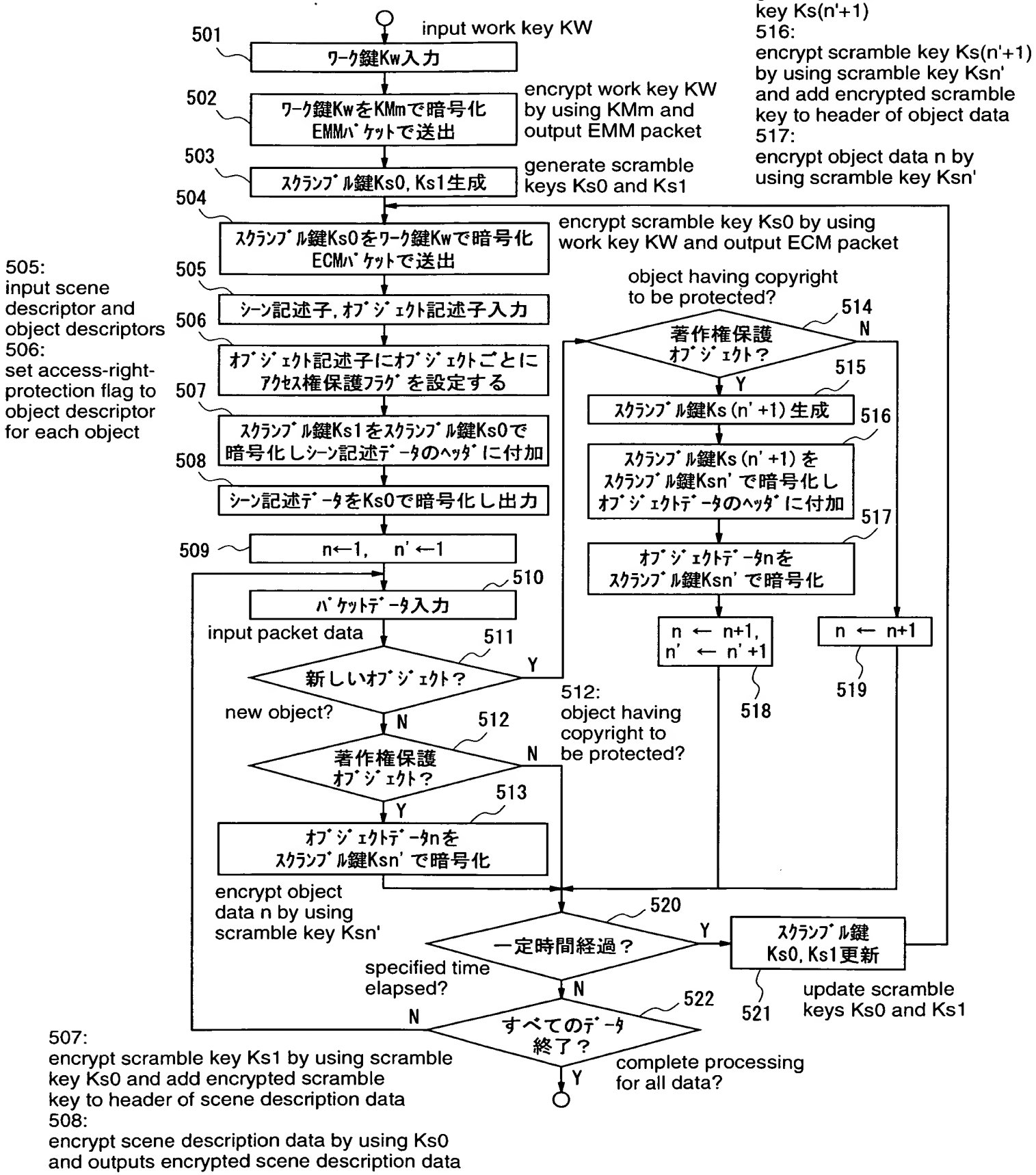
【図3】 Figure 3


(a)
scene description data
object data 1
object data 2
object data 5
object data 1
object data 2
シーン記述データ
オブジェクトデータ1
オブジェクトデータ2
オブジェクトデータ5
オブジェクトデータ1
オブジェクトデータ2
....
Dsd
ED01
ED02
ED05
MB
multiplexed bit stream
MB：多重ビットストリーム
(b)
scene description data
object data 1
object data 2
object data 5
object data 1
object data 2
シーン記述データ
オブジェクトデータ1
オブジェクトデータ2
オブジェクトデータ5
オブジェクトデータ1
オブジェクトデータ2
....
SB
SB：ビットストリーム暗号
scrambled bit stream

【図4】 Figure 4


SD
scene descriptor
シーン記述子：
OD1
OD2
OD3
OD4
OD5
A1
21
22
A2
26
23
A3
24
25
2Dオブジェクト {
ビデオオブジェクト {オブジェクト記述子1}
オーディオオブジェクト {オブジェクト記述子2}
2Dオブジェクト {
テキストオブジェクト {"Let's Start"}
ビデオオブジェクト {オブジェクト記述子3}
2Dオブジェクト {
ビデオオブジェクト {オブジェクト記述子4}
ビデオオブジェクト {オブジェクト記述子5}
}
}
}
2D object {
video object {object descriptor 1}
audio object {object descriptor 2}
2D object {
text object {"Let's Start"}
video object {object descriptor 3}
2D object {
video object {object descriptor 4}
video object {object descriptor 5}
OD1
オブジェクト記述子1：
オブジェクト番号：1
ストリームタイプ：MPEG4ビデオ
アクセス権情報：コピー禁止
オブジェクト記述子3：
OD3
オブジェクト番号：3
ストリームタイプ：MPEG4ビデオ
アクセス権情報：コピー禁止
オブジェクト記述子5：
OD5
オブジェクト番号：5
ストリームタイプ：MPEG4ビデオ
アクセス権情報：コピー禁止
OD2
オブジェクト記述子2：
オブジェクト番号：2
ストリームタイプ：MPEG4オーディオ
アクセス権情報：コピー可
オブジェクト記述子4：
OD4
オブジェクト番号：4
ストリームタイプ：MPEG4オーディオ
アクセス権情報：コピー可
object descriptor 1 :
object number : 1
stream type : MPEG4 video
access right information : copying "unauthorized"
object descriptor 3 :
object number : 3
stream type : MPEG4 video
access right information : copying "unauthorized"
object descriptor 5 :
object number : 5
stream type : MPEG4 video
access right information : copying "unauthorized"
object descriptor 2 :
object number : 2
stream type : MPEG4 audio
access right information : copying "authorized"
object descriptor 4 :
object number : 4
stream type : MPEG4 audio
access right information : copying "authorized"

【図5】 Figure 5



505:
input scene descriptor and object descriptors

506:
set access-right-protection flag to object descriptor for each object

507:
encrypt scramble key Ks1 by using scramble key Ks0 and add encrypted scramble key to header of scene description data

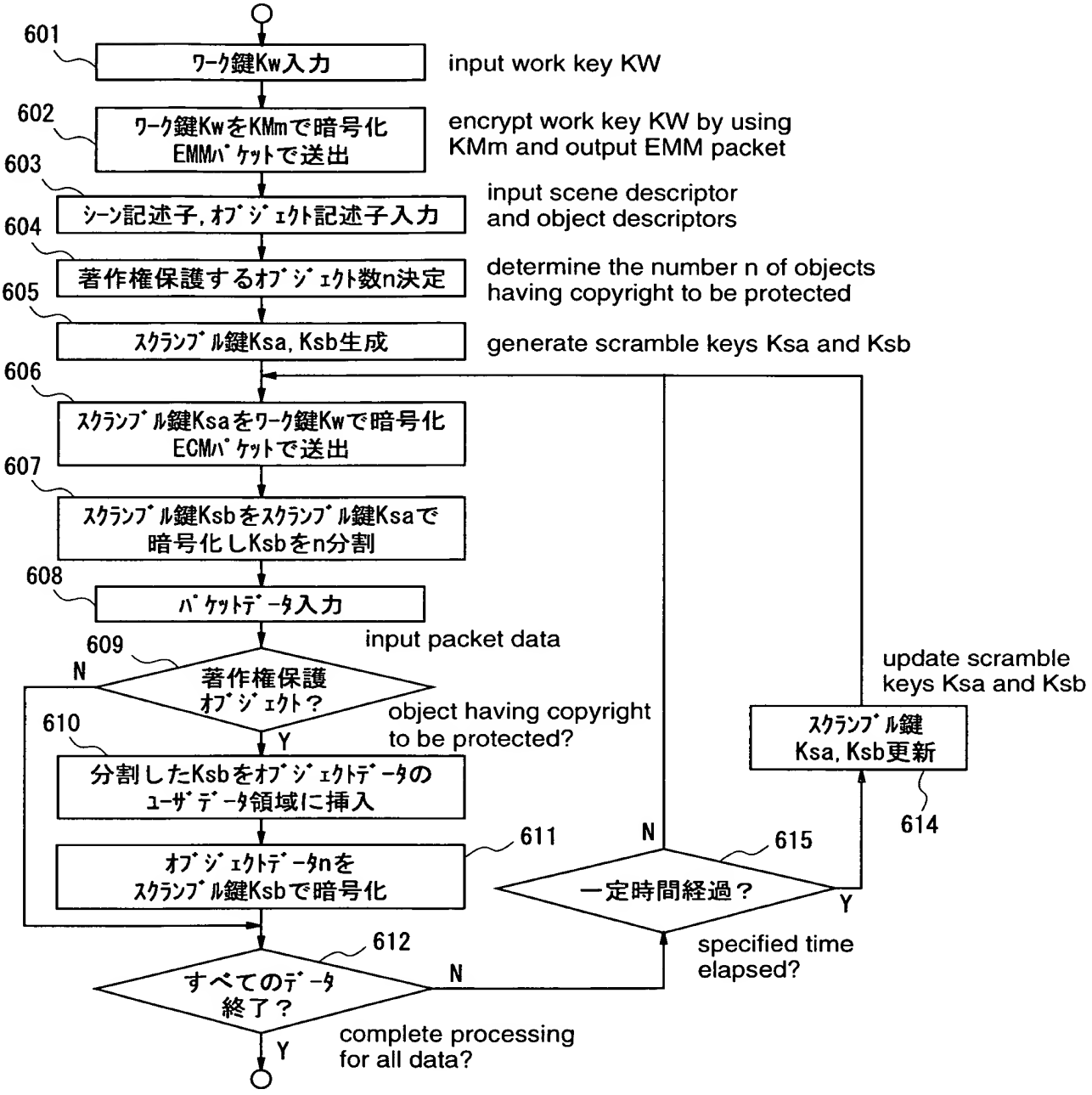
508:
encrypt scene description data by using Ks0 and outputs encrypted scene description data

515:
generate scramble key Ks(n'+1)

516:
encrypt scramble key Ks(n'+1) by using scramble key Ksn' and add encrypted scramble key to header of object data

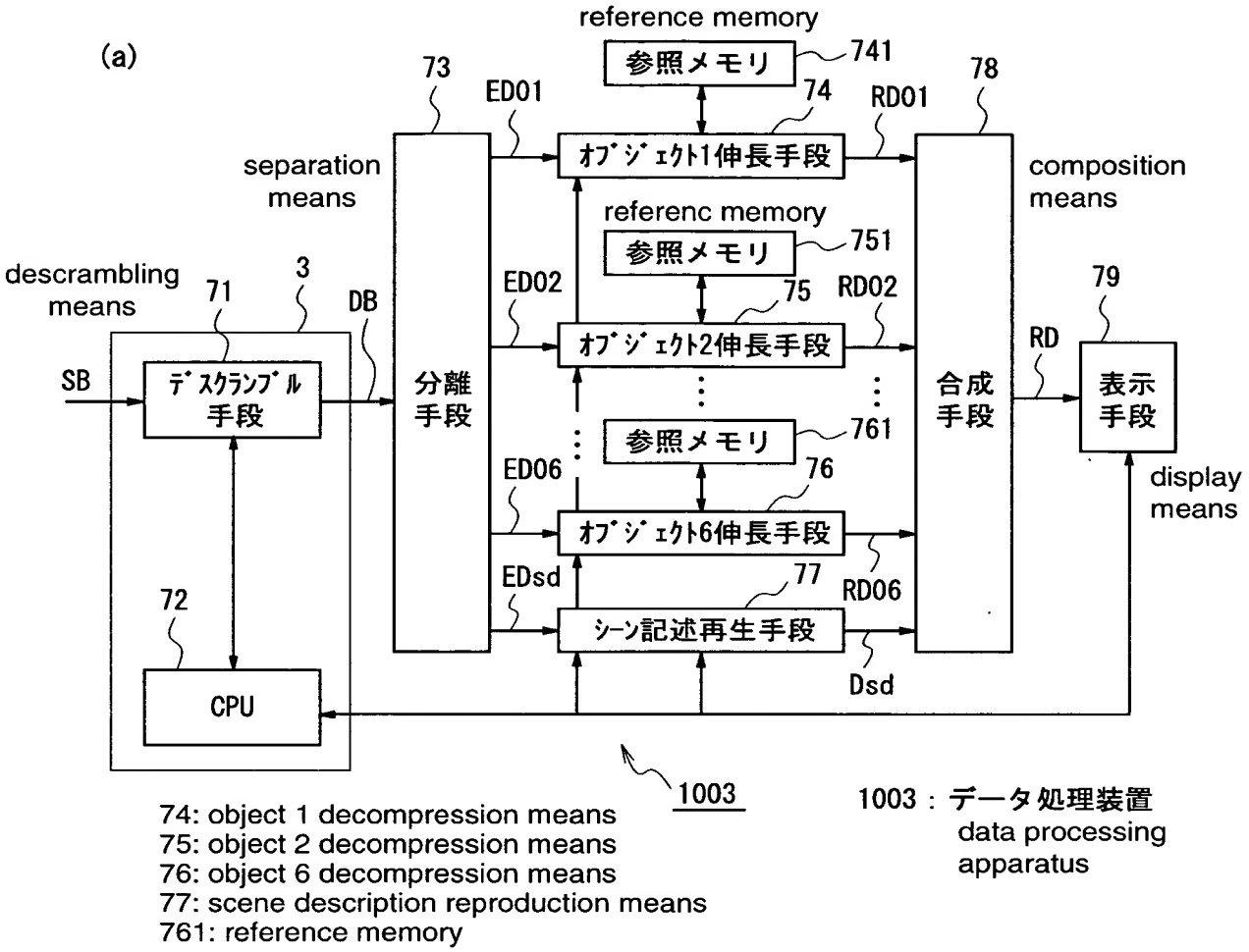
517:
encrypt object data n by using scramble key Ksn'

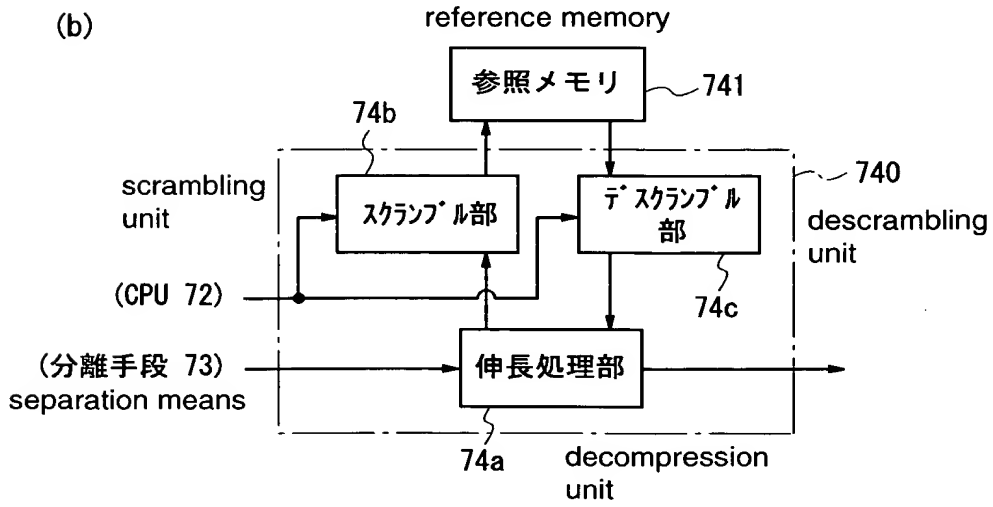
【図6】 Figure 6



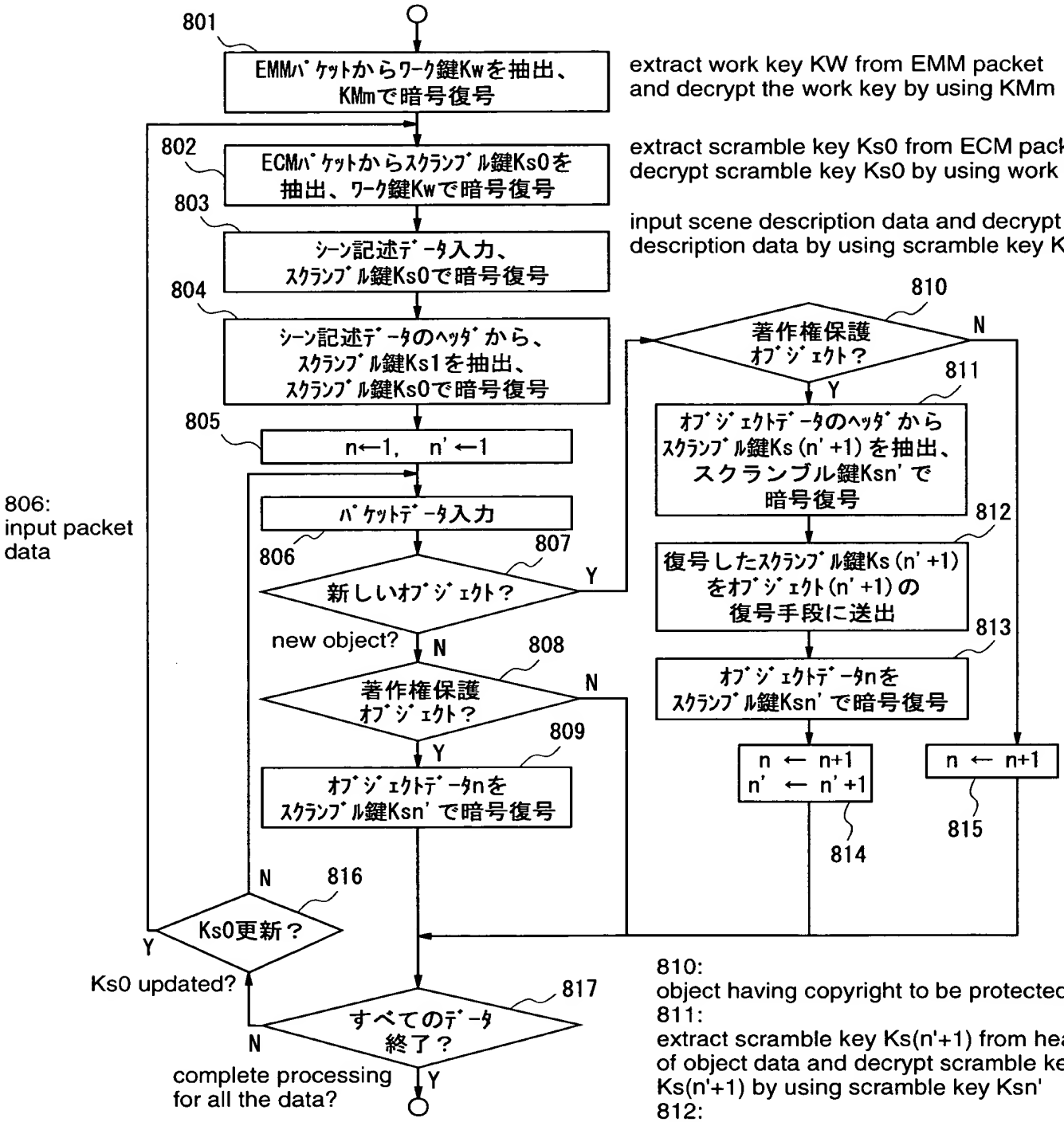
606:
encrypt scramble key Ksa by using work key KW and output ECM packet
607:
encrypt scramble key Ksb by using scramble key Ksa and divide encrypted scramble key Ksb into n-divided parts
610:
insert divided Ksb into user data regions of object data
611:
encrypt object data n by using scramble key Ksb

【図7】 Figure 7


(a)
reference memory
参照メモリ
741
73
ED01
74
RD01
78
separation means
オブジェクト1伸長手段
composition means
referenc memory
参照メモリ
751
descrambling means
71
3
DB
ED02
75
RD02
79
RD
SB
デスクランブル手段
分離手段
オブジェクト2伸長手段
合成手段
表示手段
参照メモリ
761
ED06
76
display means
オブジェクト6伸長手段
EDsd
77
RD06
72
シーン記述再生手段
CPU
Dsd
1003
74: object 1 decompression means
75: object 2 decompression means
76: object 6 decompression means
77: scene description reproduction means
761: reference memory
1003 : データ処理装置
data processing apparatus


(b)
reference memory
参照メモリ
741
74b
740
scrambling unit
スクランブル部
デスクランブル部
descrambling unit
(CPU 72)
74c
(分離手段 73)
separation means
伸長処理部
74a
decompression unit

【図8】 Figure 8



804:
extract scramble key Ks1 from header of scene description data and decrypt scramble key Ks1 by using scramble key Ks0

808:
object having copyright to be protected?

809:
decrypt object data n by using scramble key Ksn'

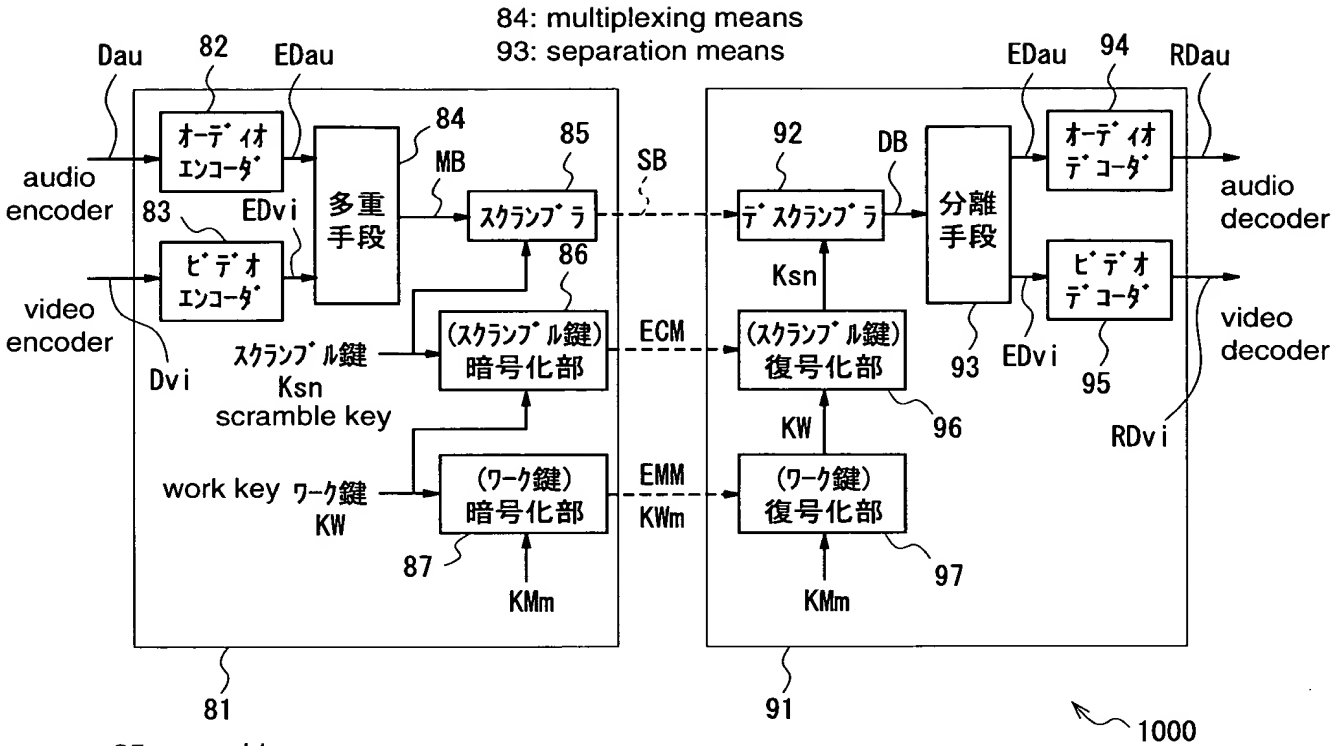
810:
object having copyright to be protected?

811:
extract scramble key Ks(n'+1) from header of object data and decrypt scramble key Ks(n'+1) by using scramble key Ksn'

812:
output decrypted scramble key Ks(n'+1) to descrambling means for object (n'+1)

813:
decrypt object data n by using scramble key Ksn'

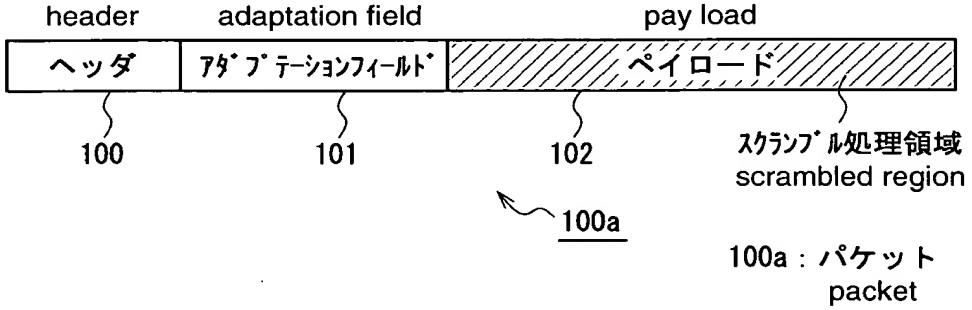
【図9】 Figure 9



85: scrambler
86: (scramble key) encryption unit
87: (work key) encryption unit
92: descrambler
96: (scramble key) decryption unit
97: (work key) decryption unit

81：データ送出側装置
91：データ受信側装置
1000：データ送受信システム
81: data transmission-side apparatus
91: data receiving-side apparatus
1000: data transmission/receiving system

【図10】 Figure 10



【図11】 Figure 11